1459

Curves and exponential series in the theory of noncommutative formal groups.

E.J.Ditters

Curves and exponential series in the theory
of noncommutative formal groups.

Aan Alexa
Willem Everhard
Elisabet

Promotor: Prof.Dr.A.H.M.Levelt

Curves and exponential series in the theory of noncommutative formal groups.

Proefschrift

ter verkrijging van de graad van doctor
in de wiskunde en natuurwetenschappen
aan de katholieke universiteit te Nijmegen
op gezag van de rector magnificus Mr. S.F.L.baron van Wijnbergen,
hoogleraar in de faculteiten der rechtsgeleerdheid
en der sociale wetenschappen
volgens besluit van de senaat
in het openbaar te verdedigen
op woensdag 25 juni des namiddags te 4 uur.

door

Engelbertus Joseph Ditters
geboren te Rotterdam

1969

Stencildruk: Faculteit der Wiskunde en Natuurwetenschappen.

L'auteur espère, que Monsieur Pierre Gabriel pourra retrouver dans cette étude la justification de sa patience et de son encouragement.
L'auteur remercie Monsieur Pierre Cartier d'avoir bien voulu lire une version antérieure des trois premiers chapitres.
L'auteur leur doit plusieurs suggestions importantes. Cependant ils ne sont pas responsables pour les imperfections éventuelles du présent travail.

CONTENTS

INTRODUCTION

The main aim of this study is to give full proofs for the theorem and other assertions that are stated in a Note of the author in the Comptes Rendus (C.R. Acad. Sc. Paris, t 268, série A, 1969, 580-582).
The object of this study is the theory of formal groups, or equivalently, of formal cogroups, defined over arbitrary fields. Making use of continuous linear dualisation, it amounts to the same to study enveloping algebras of Liealgebras, if the groundfield has characteristic zero, shortly, in the $\chi = 0$ case, or to study hyperalgebras, if the groundfield has positive characteristic, shortly, the $\chi > 0$ case. For categorical reasons we will speak of groupcoalgebras instead of hyperalgebras.
It goes without saying that each author on that field has to acknowledge the enormous amount of results, obtained by J.A. Dieudonné in a series of papers, published between 1954 and 1959. Consequently, a study that goes back to basic questions in this field asks for motivation. In order to do this we introduce some notions and sketch the main results of the present study.
Our main tool will be the concept of curve. If B is a formal cogroup, i.e. the affine algebra of a formal group and if B^χ is its continuous linear dual, a curve ϕ in B^χ is by definition a continuous homomorphism of k-algebras such that the following diagram commutes:

$$\begin{array}{ccc} B & \xrightarrow{\phi} & k[[t]] \\ & {\scriptstyle\varepsilon}\searrow \quad \swarrow{\scriptstyle\varepsilon'} & \\ & k & \end{array}$$

(ε is the canonical augmentation (counit) and ε' is the residu map).
We equally study finite curves of order i, where $k[[t]]$ has to be replaced by $k[[t]]/(t^{i+1})$. As is generally known, the case i = 1 gives the Liealgebra of the formal cogroup B.

The set of curves in B^* has a groupstructure, functorial in B and it turns out that this functor is representable in the category of groupcoalgebras. The object representing this functor will be denoted UNG. This concept of curve agrees with the notion of curve, introduced for commutative formal groups by P. Cartier [9]. These notions and preliminaries are introduced in Chapter I.

In the $\chi = 0$ case, the fundamental role of the exponential series in the connection of Liealgebras and local Liegroups is generally known. The exponential series defines in a natural way the exponential curve. In the $\chi > 0$ case, it turns out that there exists a curve, called E-pure curve, with analoguous properties. This curve is defined in terms of non commutative universal polynomials $E_0, E_1, \ldots$ In Chapter II, the definition, existence and rationality over the prime field of these polynomials are established.

In Chapter III we define the notion of E-pure curve and we study the analogy between the exponential curve and the E-pure curve. In the $\chi = 0$ case, the exponential curve defines the groupcoalgebra $U = k[\underline{X}]$, $X \longmapsto X \otimes 1 + 1 \otimes X$. In a similar way, the E-pure curve defines in the $\chi > 0$ case a groupcoalgebra, denoted NEG. In contrast to the non unicity of the polynomials $E_0, E_1, \ldots$, this NEG is a canonical object in the category of groupcoalgebras. In the $\chi = 0$ case, every curve is an infinite product of exponential curves. As far as the author knows, this useful although simple fact concerning the set of k-algebra homomorphisms $B \to k[[t]]$ has never been explicitly stated. It has its counterpart in the $\chi > 0$ case: Each curve is an infinite product of E-pure curves. As P. Gabriel kindly did observe to the author, P. Cartier had obtained this for curves in commutative formal groups. This decomposition theorem gives rise to operations which generalise the structure of p-Liealgebras. Using these operations one easily recovers the Campbell-Hausdorff-Dieudonné theorem:

Each curve in the $\chi > 0$ case is itself an E-pure curve.

As P. Cartier observed, [Math. Reviews 20-930] a construction of the UNG and the NEG can already be found in Dieudonné's paper [5]. In the approach of Dieudonné, the important technical tool is the structural base for a hyperalgebra, which can be considered as a generalisation of our notion of curve. These structural bases however did not enable him to introduce the groupstructure on the set of curves, which is essential in the present study. A consequence is that this groupstructure can be used to specialize the notion of higher derivation (semiderivation) to the notion of E-pure semiderivation.

In Chapter IV it is indicated that the theory of E-pure semiderivations gives the same functor, that classifies the affine commutative unipotent groupschemes over a perfect field. It is shown that if k is not perfect, the formal cogroups of bounded height are still determined up to isomorphism by the set of E-pure semiderivations of their Cartierduals. Finally some open questions arising from this study have been stated.

CONVENTIONS

Unless otherwise explicitly stated, a ring is always meant to be a commutative associative unitary ring. If A is a ring, then an A-algebra is always meant to be a commutative associative unitary A-algebra. Each homomorphism of rings will be unitary. k always will denote a field of characteristic $\chi(k)$. We write 0 instead of 0_k.

Iff is used as an abbreviation for "if and only if".

$\mathbb{Z}$ is the ring of integers and $\mathbb{Q}$ is its field of quotients.

Alg_k is the category of k-algebras, $NAlg_k$ is the category of associative unitary, not necessarily commutative k-algebras.

If C is a category, we write $C(X,Y)$ instead of $Hom_C(X,Y)$.

$\delta_{a,b}$ always will denote the Kronecker symbol.

For typographical reasons we sometimes write fx for f(x).

The free non commutative associative k-algebra, generated by a set $\{X_i\}_{i \in S}$ of indeterminates, indexed by S, will be denoted by $k\langle X_i \rangle_{i \in S}$. If S is denumerable, we write $k\langle X_i \rangle_{i \in S} = k\langle X_0, X_1, \ldots \rangle$. If S is finite, we write $k\langle X_i \rangle_{i \in S} = k\langle X_0, \ldots, X_n \rangle$ if S has n+1 elements.

If A is a topological ring and $\{x_i\}_{i \in S}$ is a set of elements of A, then $(x_i)_{i \in S}$ will denote the closure of the ideal of A, generated by the x_i.

In general the letters S and T will be used to denote (suitably chosen) index sets.

LIST OF SOME SYMBOLS AND DEFINITIONS

CHAPTER I

Preliminaries

In order to make the exposition more selfcontained we recollect in this chapter the basic definitions and properties. The basic references for this chapter are:

1. P. Gabriel, SGAD '63-'64 Exp VIIA and VIIB referred to as PGA and PGB.
2. P. Cartier, Séminaire Sophus Lie, 2^{e} année, referred to as PCL.

§1 Formal cogroups.

1.1.1. Definition. [PGB 0.1]. A topological ring A is called pseudocompact, if A is separated and complete and admits a fundamental system of neighborhoods of zero consisting of ideals having finite colength over A.

1.1.2. Definition. [PGB 0.2]. Let A be a pseudocompact ring. A topological unitary A-module M is called pseudocompact, if M is separated and complete and admits a fundamental system of neighborhoods of zero consisting of A-submodules having finite colength over A.

1.1.3. Definition. [PGB 0.4]. Let A be a pseudocompact ring. A topological A-algebra B is called profinite if B is pseudocompact as an A-module.
It then follows that B itself is a pseudocompact ring. If k is a field, then k is a pseudocompact ring and a profinite k-algebra if k has discrete topology.

1.1.4. The profinite A-algebras constitute a category, denoted Al_A, if one requires the morphisms in Al_A to be continuous morphisms of A-algebras. Al_A has a cofinal object, A, and projective and finite inductive limits.

[PGB 0.4.1]. We recall the construction of $A \underset{k}{\perp} B$ in Al_k. Let $\{A_\alpha\}_{\alpha \in S}$ and $\{B_\beta\}_{\beta \in T}$ be fundamental systems of neighborhoods of zero in A and B, then $A \underset{k}{\perp} B$, denoted $A \hat{\otimes} B$ is given by $A \hat{\otimes} B = \varprojlim_{\alpha,\beta} {}^{A}/_{A_\alpha} \otimes {}^{B}/_{B_\beta}$, provided with the usual lim-topology. The structure of k-algebra on $A \otimes B$ is given by $a_1 \hat{\otimes} b_1 \cdot a_2 \hat{\otimes} b_2 = a_1 a_2 \hat{\otimes} b_1 b_2$.

1.1.5. Definition. $A \in Al_k$ is called a formal cogroup over k if $Al_k(A,-)$ is a groupfunctor. If A is a formal cogroup and is local as a k-algebra, A is called an infinitesimal cogroup.

1.1.6. Let $A \in Al_k$ be a formal cogroup. In view of (1.1.4) it is known [PGB 2.1], that the cogroupstructure on A is given by a morphism $d : A \to A \hat{\otimes} A$ in Al_k, called diagonal, satisfying C1, C2, C3 below:

C1 d is coassociative.

C2 There exists a morphism $\varepsilon : A \to k$ in Al_k, necessarily unique, called augmentation or counit, such that the compositions $A \xrightarrow{d} A \hat{\otimes} A \xrightarrow{1 \hat{\otimes} \varepsilon} A \hat{\otimes} k \xrightarrow{\sim} A$ and $A \xrightarrow{d} A \hat{\otimes} A \xrightarrow{\varepsilon \hat{\otimes} 1} k \hat{\otimes} A \xrightarrow{\sim} A$ are the identity morphisms on A.

C3 There exists a morphism $c : A \to A$ in Al_k, necessarily unique, called antipodism or inversion, such that the two composite morphisms $A \xrightarrow{d} A \hat{\otimes} A \xrightarrow{c \hat{\otimes} 1} A \hat{\otimes} A \xrightarrow{m} A$ and $A \xrightarrow{\varepsilon} k \xrightarrow{\eta} A$ are equal. Here m (multiplication) and η (unit or coaugmentation) define the structure of k-algebra on A.

1.1.7. Convention. Like customary in dealing with algebras, we say: A is a formal cogroup over k instead of the couple (A,d) is a formal cogroup over k. The morphisms d,m,c,η,ε will be called structural. Unlabelled arrows in diagrams will always refer to structural morphisms if no confusion can occur.

1.1.8. The formal cogroups of Al_k constitute a category CAl_k if one requires the morphisms of CAl_k to be morphisms in Al_k that are compatible with the diagonals, i.e. $f \in CAl_k(A,B)$ must satisfy: the diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ A \hat{\otimes} A & \xrightarrow[f \hat{\otimes} f]{} & B \hat{\otimes} B \end{array}$$

is commutative. The infinitesimal formal cogroups form a subcategory of CAl_k, denoted $ICAl_k$. An object $A \in CAl_k$ is called commutative or abelian if the diagonal is cocommutative, equivalently, if $Al_k(A,-)$ is a commutative groupfunctor.

1.1.9. Notation and Definition. Let $A \in CAl_k$. We put $I_A = \mathrm{Ker}\{\varepsilon : A \to k\}$. If $A \in ICAl_k$ and $\chi(k) = p > 0$ we say: A has height $\leq n$ if $x \in I_A$ implies $x^{p^n} = F^n x = 0$. If there exists no integer n such that A has height $\leq n$, A has infinite height [PGB 4.1.2].

1.1.10. Examples and Remarks.

a. $A = k[[t]]$. $dt = t \hat{\otimes} 1 + 1 \hat{\otimes} t$. A has (t)-adic topology. $A \in ICAl_k$ and A is called the additive formal cogroup. $A = k[[t]]$, $dt = t \hat{\otimes} 1 + t \hat{\otimes} t + 1 \hat{\otimes} t$, A has (t)-adic topology. $A \in ICAl_k$ and A is called the multiplicative formal cogroup. A formal cogroup A such that A is a formal powerseries ring in n indeterminates provided with the I_A-dic topology is called a Dieudonné formal cogroup.

b. Let G be an algebraic group over k and let A be the completion of the local ring of the neutral element of G with respect to the I_A-dic topology. Then in a natural way $A \in ICAl_k$.
A is noetherian as a k-algebra.

c. Let k be perfect, $\chi(k) = p > 0$. If Spec A is a finite k-groupscheme and the underlying topological space is a point, then $A \in ICAl_k$

(discrete topology) and A has finite height. [theorem of Cartier: A is even a truncated powerseries ring].

d. The necessity of extending the category of noetherian k-algebras to profinite k-algebras is clearly shown by the concept and extensive use of recursive abelian groups in J. Dieudonné [7, formula (25)]. Denoting Alf_k the category of finite k-algebras one has: Al_k is the Pro-category of Alf_k [PGB 0.4.2] and if $\chi(k) = p > 0$, each object A in $ICAl_k$ is the projective limit of the formal cogroups $A/I_A^{(p^n)}$ which are finite if A is noetherian [PGB 4.4.2].

1 §2 Coalgebras and Groupcoalgebras.

1.2.1. Definition. [PGA 3.1]. Let A be a ring. An A-coalgebra C is a couple (C,d) consisting of an A-module C together with an A-linear map $d : C \to C \otimes_A C$, called diagonal, satisfying Ca1, Ca2:

Ca1 d is cocommutative and coassociative.

Ca2 There exists an A-linear map $\varepsilon : C \to A$, necessarily unique, called augmentation or counit, such that the composite maps $C \xrightarrow{d} C \otimes_A C \xrightarrow{\varepsilon \otimes 1} A \otimes_A C \xrightarrow{\sim} C$ and $C \xrightarrow{d} C \otimes_A C \xrightarrow{1 \otimes \varepsilon} C \otimes_A A \xrightarrow{\sim} C$ are the identity maps on C.

Following (1.1.7) we speak of the A-coalgebra C instead of the A-coalgebra (C,d) and use the same convention with respect to diagrams.

1.2.2. The A-coalgebras form a category $Coalg_A$ if one requires the morphisms in $Coalg_A$ to be A-linear maps that are compatible with the diagonal and augmentation, i.e. $f \in Coalg_A(C,D)$ iff f is A-linear and the diagrams

$$\begin{array}{ccc} C & \xrightarrow{f} & D \\ \downarrow & & \downarrow \\ C \otimes_A C & \xrightarrow{f \otimes f} & D \otimes_A D \end{array} \qquad \text{and} \qquad \begin{array}{ccc} C & \xrightarrow{f} & D \\ & \searrow \quad \swarrow & \\ & A & \end{array} \qquad \text{commute.}$$

Coalg_A has a final object, A, and finite products [PGA 3.1].

For convenience we recall that for (C,d) and (D,d') in Coalg_A one has:

$C \underset{A}{\amalg} D \simeq (C \otimes_A D, d'')$, where d'' is the composite map:

$$C \otimes_A D \xrightarrow{d \otimes d'} C \otimes_A C \otimes_A D \otimes_A D \xrightarrow{1 \otimes \sigma \otimes 1} C \otimes_A D \otimes_A C \otimes_A D,$$

$\sigma(c \otimes d) = d \otimes c$.

If $A \to A'$ is a morphism in Alg_Z and $C \in \mathrm{Coalg}_A$, then $C \otimes_A A' \in \mathrm{Coalg}_{A'}$, in a natural way.

1.2.3. Definition. $G \in \mathrm{Coalg}_A$ is called a groupcoalgebra over A if $\mathrm{Coalg}_A(-,G)$ is a groupfunctor. If $\mathrm{Coalg}_A(-,G)$ is a commutative groupfunctor, we call G an abelian groupcoalgebra or bialgebra.

1.2.4. Let G be a groupcoalgebra over k. In view of (1.2.2) it is known [PGA 3.2], that the groupstructure is given by a morphism $m : G \otimes G \to G$ in Coalg_k, called multiplication, satisfying GCa1, GCa2, GCa3 below.

GCa1 m is associative.

GCa2 There exists a morphism $\eta : k \to G$ in Coalg_k, necessarily unique, called unit map or coaugmentation such that the composite morphisms $G \xrightarrow{\sim} G \otimes k \xrightarrow{1 \otimes \eta} G \otimes G \xrightarrow{m} G$ and $G \xrightarrow{\sim} k \otimes G \xrightarrow{\eta \otimes 1} G \otimes G \xrightarrow{m} G$ are the identity map on G.

GCa3 There exists a morphism $c : G \to G$ in Coalg_k, necessarily unique, called antipodism or inversion, such that the two composite morphisms $G \xrightarrow{d} G \otimes G \xrightarrow{c \otimes 1} G \otimes G \xrightarrow{m} G$ and $G \xrightarrow{\varepsilon} k \xrightarrow{\eta} G$ are equal.

1.2.5. Morphisms with the same name will always be denoted by the same letter. (1.2.4), (1.2.1) and (1.1.6). We recall [PGA 3.2] that (m,η) defines on the groupcoalgebra G a structure of associative unitary k-algebra which is commutative if G is abelian. d and ε then are unitary homomorphisms

of k-algebras. $c : G \to G^{opp}$ is an isomorphism onto the opposite algebra, thus satisfies $c(g_1g_2) = c(g_2)c(g_1)$. The k-groupcoalgebras constitute a category $GCoalg_k$ if one requires the morphisms in $GCoalg_k$ to be morphisms in $Coalg_k$ which are compatible with the multiplication, i.e.
$f \in GCoalg_k(G,H)$ iff $f \in Coalg_k(G,H)$ and

$$\begin{array}{ccc} G \otimes G & \xrightarrow{f \otimes f} & H \otimes H \\ \downarrow & & \downarrow \\ G & \xrightarrow[f]{} & H \end{array}$$

commutes. The abelian groupcoalgebras constitute a subcategory denoted Ab_k.

1.2.6. Examples.

a. For $0 \leq n \leq \infty$ let T_n^* be the k-vectorspace $\bigotimes_{i=0}^{n} k\, t_i$, $dt_i = \sum_{\mu+\nu=i} t_\mu \otimes t_\nu$, $\varepsilon(t_0) = 1$, $\varepsilon(t_i) = 0$ if $i > 0$. Then $T_n^* \in Coalg_k$ for every n and $T^* = T_\infty^*$ is called the straightline coalgebra. $T^* \in Ab_k$ if m is given by $m(t_i \otimes t_j) = \binom{i+j}{i} t_{i+j}$. T^* will appear to be the Cartierdual of the additive formal cogroup (cf. 1§3 below).

b. Let Spec A be an affine commutative k-groupscheme, then $A \in Ab_k$ in a natural way.

c. Let $\mathfrak{g}$ be a k-liealgebra, $\chi(k) = 0$ and let $U(\mathfrak{g})$ be the enveloping algebra. Then $U(\mathfrak{g}) \in GCoalg_k$ [PGA 3.2.2].

d. Let $\chi(k) = p > 0$ and $\mathfrak{g}$ be a p-liealgebra over k. Then the restricted enveloping algebra $U_p(\mathfrak{g}) \in GCoalg_k$ [PGA 5.4].

e. Let $A \in CAl_k$ and let A^* be the continuous k-linear dual of A. Then $A^* \in GCoalg_k$ in a natural way. This phenomenon is known as Cartierduality.

f. Let $H = k[X_0, X_1, \ldots]$ be the (commutative) polynomialring in the indeterminates X_i, $i \geq 0$. Use the hyperexponential series [3, formulae

16 and 18] in order to define $d : H \to H \otimes H$,

$$dX_i = X_i \otimes 1 + 1 \otimes X_i + \sum_{1<k<p^i} E_k(X) \otimes E_{p^i-k}(X).$$

Then H has a natural structure of k-bialgebra (cf. 3.1.5 below).

In an analoguous way one defines the Witt bialgebra [3, formula (30)].

g. The universal non commutative groupcoalgebra Z and the exponential groupcoalgebras U and A. (1.2.7 sqq),

1.2.7. Consider the k-algebra $Z = k\langle Z_1, Z_2, \ldots\rangle$ in a denumerable set of indeterminates Z_i. Put by definition $Z_0 = 1$. Define $d \in NAlg_k(Z, Z \otimes Z)$ by $dZ_i = \sum_{\mu+\nu=i} Z_\mu \otimes Z_\nu$ and $\varepsilon \in NAlg_k(Z,k)$ by $\varepsilon(Z_i) = 0$ if $i > 0$. We claim: $G \in GCoalg_k$. Likewise: let Z_{com} be the largest commutative quotient of Z, then $Z_{com} \in Ab_k$. [8, cor 2].

One verifies without difficulty that the pair (Z,d) is a k-coalgebra and that the structure morphisms $m : Z \otimes Z \to Z$ and $\eta : k \to Z$ are morphisms in $Coalg_k$. In order to show the existence of the antipodism $c : Z \to Z$ in $Coalg_k$ we first observe that if the antipodism c exists, it must satisfy $m \circ c \otimes 1 \circ d = \eta \circ \varepsilon$ and applying this to $Z_i \in Z$, we have

$$(1.1) \qquad \sum_{\mu+\nu=i} c(Z_\mu)Z_\nu = \delta_{oi} \text{ for all } i \geq 0.$$

Using the set of equations (1.1) we can define $c : Z \to Z^{opp}$ as an isomorphism of k-algebras. By the canonical bijection $Z^{opp} \to Z$ as sets, we have a map $c : Z \to Z$, and it is a trivial verification that $m \circ c \otimes 1 \circ d = \eta \circ \varepsilon$. In order to show that $c \in Coalg_k(Z,Z)$ we give a shortcircuit, observed by A.H.M. Levelt, of the original proof: Consider the formal powerseries rings $Z[[t]]$ and $(Z \otimes Z)[[t]]$ denoted $\overline{Z}$ and $\overline{Z \otimes Z}$, and the morphism in $NAlg_k$

$$\theta : \overline{Z} \otimes \overline{Z} \to \overline{Z \otimes Z} \quad , \quad d : \overline{Z} \to \overline{Z \otimes Z}$$

defined by

$$\Sigma z_i t^i \otimes \Sigma w_j t^j \xrightarrow{\theta} \Sigma\Big(\sum_{i+j=n} z_i \otimes w_j\Big)t^n, \quad \Sigma z_i t^i \xrightarrow{d} \Sigma (dz_i)t^i.$$

It follows immediately from (1.1) that $(\Sigma\ c(Z_\nu)t^\nu).(\Sigma\ Z_\mu t^\mu) = 1$. Because d is a morphism in $NAlg_k$, we have:

$$(\Sigma\ dc(Z_\nu)t^\nu).\ \Sigma_\mu\ (\Sigma_{i+j=\mu}\ Z_i \otimes Z_j)t^\mu = 1 = (\Sigma\ dc(Z_\nu)t^\nu)\ \theta\ (\Sigma\ Z_i t^i \otimes \Sigma\ Z_j t^j).$$

On the other hand: $\theta(\Sigma\ c(Z_i)t^i \otimes \Sigma\ c(Z_j)t^j).\theta\ (\Sigma\ Z_i t^i \otimes \Sigma\ Z_j t^j) = 1$.

From these two relations we deduce:

$$\Sigma\ dc(Z_\nu)t^\nu = \theta\ (\Sigma\ c(Z_i)t^i \otimes \Sigma\ c(Z_j)t^j)$$

$$= \Sigma_\nu\ (\Sigma_{i+j=\nu}\ c(Z_i) \otimes c(Z_j))t^\nu$$

i.e.: $dc(Z_\nu) = \Sigma_{i+j=\nu}\ c(Z_i) \otimes c(Z_j) = c \otimes c \circ d\ (Z_\nu)$ for all $\nu \geq 0$.

It now follows without difficulty that if $dc(Z_\nu) = c \otimes c \circ d\ (Z_\nu)$ for the generators Z_ν, then $dc = c \otimes c \circ d$, i.e. c is a morphism of coalgebras, and $Z \in GCoalg_k$.

1.2.8. Definition. The object $Z \in GCoalg_k$ will be called the universal non-commutative groupcoalgebra over k. We abbreviate this by: Z is the UNG_k. Note that the structural morphisms of Z are such that Z is already defined over Z.

1.2.9. Let Z be the UNG_k. For every integer $i \geq 1$, $Z(i) = k\langle Z_1,\ldots,Z_i\rangle \subset Z$ is a subgroupcoalgebra of Z. This is clear from the particular form of the structural morphisms of Z.

1.2.10. Let Z be the UNG_k. Define the weightfunction $\omega : Z \to \mathbb{Z}$ by $\omega(Z_i) = i$, $i \geq 0$, and extend ω to the monomials in Z_i by defining $\omega(xy) = \omega(x) + \omega(y)$ if x and y are monomials. Because the set $\{M_\alpha | M_\alpha$ is a monomial in the $Z_i\}$ is a base for the k-vectorspace Z, we can uniquely write $x = \Sigma_\alpha\ \lambda_\alpha M_\alpha$, $\lambda_\alpha \in k$. We then put $\omega(x) = \max_\alpha \{\omega(M_\alpha) | \lambda_\alpha \neq 0\}$. Define $\overline{\omega} : Z \otimes Z \to \mathbb{Z}$ by $\overline{\omega}(x \otimes y) = \omega(x) + \omega(y)$. Then putting $\overline{\omega} = \omega$, we have $\omega d(x) = \omega(x)$ for every monomial x, i.e. ω is compatible with d. We define

an exhaustive ascending ω-filtration $\{H_n\}_{n\geq 0}$ on Z by $H_n = \{z \in Z | \omega(z) \leq n\}$. In the sequel we use ω and the ω-filtration $\{H_n\}_{n\geq 0}$ without further reference. We shall use the convention that the zero element $0 \in Z$ has arbitrary weight.

§3 Cartierduality.

The nice properties of Cartierduality over a groundfield are quoted from the more general exposition given in [PGB 2.2.1] and [PCL Exp 2].

Let $A \in CAl_k$ (1.1.8). The structural morphisms of A constitute the diagrams:

$$(1.2) \qquad A \xrightarrow{d} A \hat{\otimes} A \xrightarrow{m} A \quad , \quad A \xrightarrow{c} A \quad , \quad k \xrightarrow{\eta} A \xrightarrow{\varepsilon} k.$$

Let for every pseudocompact k-module L, L^* denote the k-module of continuous k-linear maps $L \to k$. By [PGB 0.3.6] we have: the canonical map $\phi : A^* \otimes A^* \to (A \hat{\otimes} A)^*$, defined by $\phi(f \otimes g)(a_1 \hat{\otimes} a_2) = f(a_1)g(a_2)$, is an isomorphism. Continuous dualisation then gives the diagrams:

$$(1.3) \qquad A^* \xleftarrow{d^*} A^* \otimes A^* \xleftarrow{m^*} A^* \quad , \quad A^* \xleftarrow{c^*} A^* \quad , \quad k \xleftarrow{\eta^*} A^* \xleftarrow{\varepsilon^*} k.$$

and the Cartierduality theorem says in this case:

1.3.1. Theorem (Cartier). The dualisation functor $?^*$ gives an antiequivalence $?^* : Al_k \to Coalg_k$ and an antiequivalence, equally denoted $?^*, ?^* : CAl_k \to GCoalg_k$. The structural morphisms (1.2) give the structural morphisms (1.3). The inverse functor $Mod_k(-,k) : Coalg_k \to Al_k$ or $Mod_k(-,k) : GCoalg_k \to CAl_k$ is given by $Mod_k(G,k) = \{$module of all k-linear maps $G \to k\}$.

Remark on the proof The case of exhaustively filtered groupcoalgebras is given in [PCL Exp 2§2]. The more general situation is described in [PGB 2.2.1]. In view of the duality theorem, no confusion can occur if

we denote $\mathrm{Mod}_k(G,k)$ again by G^* for we have canonical isomorphisms $G^{**} \xrightarrow{\sim} G$ if $G \in \mathrm{Al}_k$ or $G \in \mathrm{Coalg}_k$. Another way to prove the theorem is: Let Alf_k be the category of the finite dimensional k-algebras and fCoalg_k the category of the finite dimensional k-coalgebras. The anti-equivalence of the categories Alf_k and fCoalg_k is readily established [PGA 3.1.1] and can be extended to an anti-equivalence of the categories $\mathrm{Pro\text{-}Alf}_k$ and $\mathrm{Ind\text{-}fCoalg}_k$ (pro-objects and ind-objects). One then verifies that the categories $\mathrm{Pro\text{-}Alf}_k$ and Al_k, resp. $\mathrm{Ind\text{-}fCoalg}_k$ and Coalg_k are equivalent. Restricting this to the cogroupobjects of Al_k and the group-objects of Coalg_k, theorem (1.3.1) follows.

1.3.2. Definition. Let $A = \bigoplus_{\alpha \in S} k\, e_\alpha$ be a k-module. The set $\{f_\alpha\}_{\alpha \in S}$ in $\mathrm{Mod}_k(A,k)$ will be called the set of pointdistributions on the base $\{e_\alpha\}_{\alpha \in S}$ if $\langle f_\alpha, e_\beta \rangle = \delta_{\alpha,\beta}$ for $\alpha,\beta \in S$. $\langle , \rangle$ is the canonical contraction map.

1.3.3. Cartierduality is related to the topology in the following way: Let $G = \bigoplus_{\alpha \in S} k\, e_\alpha \in \mathrm{GCoalg}_k$, then $G^* = \prod_{\alpha \in S} k\, f_\alpha$ if $\{f_\alpha\}_{\alpha \in S}$ is the set of pointdistributions on the base $\{e_\alpha\}_{\alpha \in S}$. The topology on G^* is the coarsest such that for every finite subset $F \subset S$ the natural projection $\prod_{\alpha \in S} k\, f_\alpha \to \prod_{\alpha \in F} k\, f_\alpha$ is continuous. Every element of G^* can uniquely be written in the form $\sum_{\alpha \in S} \lambda_\alpha f_\alpha$, $\lambda_\alpha \in k$. An arbitrary number of the λ_α may be unequal to zero. In view of the isomorphism $G^* \hat{\otimes} G^* \xrightarrow{\sim} (G \otimes G)^*$ we can write $x \in G^* \hat{\otimes} G^*$ uniquely as $x = \sum_{\alpha,\beta \in S} \lambda_{\alpha\beta} f_\alpha \hat{\otimes} f_\beta$, and if $g_1, g_2 \in G$ we have: $\langle g_1 \otimes g_2, \sum_{\alpha,\beta} \lambda_{\alpha\beta} f_\alpha \hat{\otimes} f_\beta \rangle = \sum_{\alpha,\beta} \lambda_{\alpha\beta} \langle g_1, f_\alpha \rangle \langle g_2, f_\beta \rangle$. This sum is defined in k because almost every term is zero.

1.3.4. Definition. Let $G \in \mathrm{GCoalg}_k$. The natural ascending filtration $\{G_n\}_{n \geq 0}$ [PGB 1.3.6] on G is defined by: $G^+ = \mathrm{Ker}\,\{\varepsilon : G \to k\}$, $G \xrightarrow{\sim} k \oplus G^+$, $G_0 = \eta(k)$ and $G_{n+1} = \{x \in G \mid dx - x \otimes 1 \in G_n \otimes G^+\}$ for all $n \geq 0$.

We quote from loc.cit. the important lemma:

1.3.5. Lemma. Let $G \in GCoalg_k$ and $\{G_n\}_{n\geq 0}$ be the natural filtration on G. Then:

a $G_n = (\overline{G^*/I^{n+1}})^*$, $I = \mathrm{Ker}\,\{\varepsilon : G^* \to k\}$. $\overline{I^{n+1}}$ is the closure of I^{n+1}.

b $G^* \in ICAl_k$, i.e. G^* is local as a k-algebra iff $G = \bigcup_n G_n$.

1.3.6. Lemma. If Z is the UNG_k, then $Z^* \in ICAl_k$.

Proof. Let $\{G_n\}_{n\geq 0}$ and G^+ define the natural filtration on Z and let $\{H_n\}_{n\geq 0}$ be the ω-filtration on Z (1.2.10). In view of the foregoing lemma it suffices to prove that $H_n \subset G_n$ for every $n \geq 0$. This being clear if $n = 0$, assume that $H_\mu \subset G_\mu$ for all $\mu < n$, $n \geq 0$.
Let M be a monomial in Z, $\omega(M) = n$. From $dZ_i = \sum_{\mu+\nu=i} Z_\mu \otimes Z_\nu$ it follows: $dM = M \otimes 1 + 1 \otimes M + \sigma(M)$, $\sigma(M) \in (H_{n-1} \otimes H_{n-1}) \cap (G^+ \otimes G^+)$. Thus in view of the inductionhypothesis: $dM - M \otimes 1 \in H_{n-1} \otimes G^+ \subset G_{n-1} \otimes G^+$, i.e. $M \in G_n$.

1.3.7. Lemma. Let Z be the UNG_k, $\chi(k) = p > 0$. Then Z^* has infinite height and is not noetherian.

Proof. Put $Z = \bigoplus_{\alpha \in S} \{k M_\alpha \mid M \text{ is monomial in the } Z_\mu\}$ and let $\{f_\alpha\}_{\alpha \in S}$ be the set of pointdistributions on $\{M_\alpha\}_{\alpha \in S}$. In particular let $\langle f_\alpha, Z_1\rangle = 1$. Applying Cartierduality it follows for $n \geq 0$:

$$\langle f_\alpha^{p^n}, Z_{p^n}\rangle = \langle f_\alpha \underbrace{\hat{\otimes} \ldots \hat{\otimes}}_{p^n\text{-times}} f_\alpha, \sum Z_{\mu_1} \otimes \ldots \otimes Z_{\mu_{p^n}}\rangle = 1.$$

The domain of summation is the set of all nonnegative integer solutions of $\mu_1 + \ldots + \mu_{p^n} = p^n$. Thus Z^* has infinite height.
By (1.3.5) lemma a we have $G_1 = (\overline{Z/I^2})^*$, where $\{G_n\}_{n\geq 0}$ is the natural filtration on Z. Put $G_1^+ = G_1 \cap G^+$. An easy verification shows: $G_1^+ = \{x \in Z \mid dx = x \otimes 1 + 1 \otimes x\}$. Now $Z^* \in ICAl_k$ (1.3.6) and Z^* being

complete, we have: Z^* is generated by each set $\{m_\alpha\}_{\alpha \in T} \subset I$ such that the $m_\alpha \bmod I^2$ generate I/I^2. In view of $G_1^+ \subset G_1 = (Z'/I^2)^\wedge$ it is sufficient to show that $\dim G_1^+$ is not finite. Now observe: $\hat{\bigoplus_{n=0}^{\infty}} k\, Z_1^{p^n} \subset G_1^+$ and we are done.

1.3.8. The lemma (1.3.7) shows that [PGB theorem page 146] does not apply to $Z^\wedge$. Remarks made by P. Gabriel and P. Cartier say however that noetherian conditions are not essential and can be dropped. On the other hand the author does not know explicit references in order to deal with non noetherian cases as $Z^\wedge$. In 1§6 we therefore will prove that $Z^\wedge$ is a formal powerseries algebra over k in a denumerable set of quantities, using the concept of ordered p-bases that will prove to be a useful tool in the study of formal cogroups. For future reference we state a weak form of [PGB theorem page 146]:

1.3.9. Theorem (Dieudonné-Cartier): Let k be a perfect field, $\chi(k) = p > 0$. Let $A \in ICAl_k$. Suppose either A has finite height or A is noetherian, then A is isomorphic with the completed tensorproduct of a finite number of truncated powerseries algebras over k.

1§4 Two embedding diagrams, curves.

If $M,N \in Al_k$, $Lin_k(M,N)$ will denote the module of continuous k-linear maps $M \to N$.

1.4.1. Lemma. Let $G \in CAl_k$. Define for every $T \in Al_k$ a law of composition on $Lin_k(G,T)$, $(f,g) \mapsto fg$, as follows: If $f,g \in Lin_k(G,T)$ then fg is the composite map

$$G \to G \hat{\otimes} G \xrightarrow{f \hat{\otimes} g} T \hat{\otimes} T \to T.$$

Then: for this structure $Lin_k(G,-)$ is a covariant functor $Al_k \to NAlg_k$. If G is abelian, then $Lin_k(G,-)$ is a covariant functor $Al_k \to Alg_k$.

Remark on the proof. fg is clearly continuous. All other verifications are known and easy. $1 \in \mathrm{Lin}_k(G,T)$ is the map $G \to k \to T$.

1.4.2. Definition. Let $G \in \mathrm{CAl}_k$ and $T \in \mathrm{Al}_k$. The endomorphism functor $\mathrm{End}_G : \mathrm{Al}_k \to \mathrm{NAlg}_k$ is defined by

$$\mathrm{End}_G(T) = \mathrm{Lin}_T(G \hat{\otimes} T,\ G \hat{\otimes} T) \xrightarrow{\sim} \mathrm{Lin}_k(G, G \hat{\otimes} T)$$

and the automorphism functor $\mathrm{AlAut}_G : \mathrm{Al}_k \to \mathrm{Groups}$ by $\mathrm{AlAut}_G(T) =$ Set of invertible elements of $\mathrm{Al}_T(G \hat{\otimes} T,\ G \hat{\otimes} T) \xrightarrow{\sim} \mathrm{Al}_k(G, G \hat{\otimes} T)$.

Note that these definitions make sense, for if $T \in \mathrm{Al}_k$ then the profinite k-algebra T itself is a pseudocompact ring [PGB 0.4] and $G \hat{\otimes} T$ is obviously a profinite T-algebra [PGB 0.5].

1.4.3. Proposition. Define for every $T \in \mathrm{Al}_k$ and $G \in \mathrm{CAl}_k$ the maps:

$$\mu(G,T) : \mathrm{Lin}_k(G,T) \to \mathrm{End}_G(T)$$

$$\sigma(G,T) : \mathrm{End}_G(T) \to \mathrm{Lin}_k(G,T)$$

by commutativity of the two diagrams:

$$\begin{array}{ccc} G \hat{\otimes} G \hat{\otimes} T & \xrightarrow{1 \hat{\otimes} f \hat{\otimes} 1} & G \hat{\otimes} T \hat{\otimes} T \\ {\scriptstyle d \hat{\otimes} 1}\uparrow & & \downarrow{\scriptstyle 1 \hat{\otimes} m} \\ G \hat{\otimes} T & \xrightarrow[\mu(G,T)(f)]{} & G \hat{\otimes} T \end{array} \qquad \text{and} \qquad \begin{array}{ccc} G \hat{\otimes} T & \xrightarrow{\quad f \quad} & G \hat{\otimes} T \\ \uparrow{\scriptstyle \mathrm{can}} & & {\scriptstyle \varepsilon \hat{\otimes} 1}\downarrow \\ G \hat{\otimes} k \xrightarrow{\sim} G & \xrightarrow[\sigma(G,T)(f)]{} & G \xrightarrow{\sim} k \hat{\otimes} T \end{array}$$

then

a $\mu(G,-)$ is a monomorphism of k-algebra functors

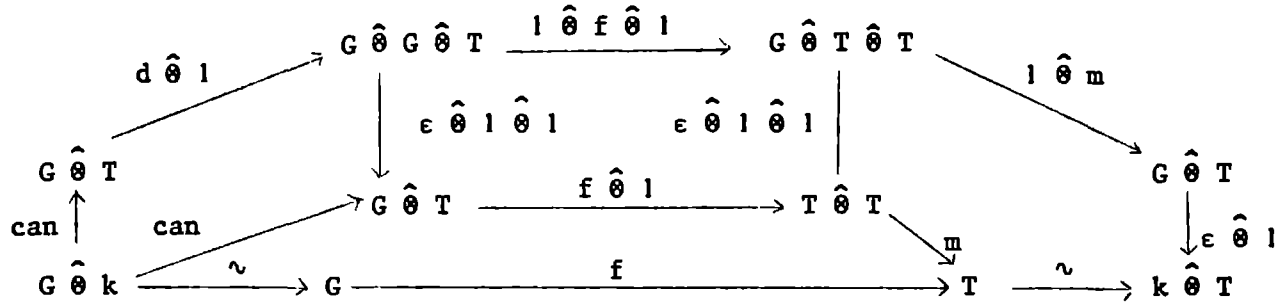
b $\sigma(G,-)$ is an epimorphism of k-module functors

c $\sigma(G,-) \circ \mu(G,-)$ is the identity functor endomorphism on $\mathrm{Lin}_k(G,-)$.

Remark on the proof. First observe that there are no topological difficulties: everything is defined with help of diagrams of continuous maps. Thus the verification is purely of algebraic nature and in dual, infinitesimal fashion (i.e. language of schemes and of deviations in the origine) stated in [PGA 2.2 and 2.3]. A full proof would fill pages of monstruous diagrams

and asks for no tricks but courage. We exhibit an innocent one:

Proof of c. The diagram



is commutative.

1.4.4. Corollary. The restriction of $\mu(G,-)$ to $Al_k(G,-)$ factorizes through $AlAut_G$, i.e.: we have a commutative diagram, functorial in $T \in Al_k$:

$$\begin{array}{ccc} Al_k(G,T) & \hookrightarrow & AlAut_G(T) \\ \downarrow & & \downarrow \\ Lin_k(G,T) & \xrightarrow[\mu(G,T)]{} & End_G(T) \end{array}$$

Proof. The elements of $Al_k(G,T)$ belong to the group of units in $Lin_k(G,T)$. Indeed,if $f \in Al_k(G,T)$, then in the group $Al_k(G,T)$ we have $f^{-1} = f \circ c$, and their product $f.(f \circ c)$ is the composition map $G \to k \to T$ which acts as the identity $1 \in Lin_k(G,T)$. Thus $\mu(G,T)f$ is a linear automorphism of $G \hat{\otimes} T$ and is moreover an endomorphism of profinite T-algebras as may easily be checked.

1.4.5. First embedding diagram: If T = k, prop. (1.4.3) gives an embedding

$$\mu(G,k) = \mu : G^{\chi} \hookrightarrow Lin_k(G,G) \tag{1.4}$$

in $NAlg_k$ where G^{χ} is the Cartierdual of G. μ admits a linear retraction $\sigma(G,k) = \sigma$, given by $\sigma(f) = \varepsilon \circ f : G \xrightarrow{f} G \to k$.

$\mu(f)$, denoted furtheron $\overline{f}$ is the composite map $G \to G \hat{\otimes} G \xrightarrow{1 \hat{\otimes} f} G \hat{\otimes} k \xrightarrow{\sim} G$.

Prop.(1.4.3) enables us to replace the Cartierproductstructure on G^* by

the composition of continuous linear endomorphisms of G.

(1.4) will be referred to as the first embedding diagram.

1.4.6. In order to arrive at the second embedding diagram we prove in this section some easy lemmata. Define for $0 \leq i \leq \infty$, T_i by $T_i = k[[t]]/(t^{i+1})$ and $T = T_\infty = k[[t]]$. Giving T_i the discrete topology if $i < \infty$ and T the (t)-adic topology, $T_i \in Al_k$ for all i and $T = \lim_{\leftarrow} T_i$.

Lemma 1. Let $\{t_j\}_{0\leq j\leq i}$ be the set of pointdistributions on the powers of t, $\{t^j\}_{0\leq j\leq i}$, satisfying $\langle t_i, t^j\rangle = \delta_{ij}$, then the Cartierdual of T_i is given by $T_i^* = \bigoplus_{j=0}^{i} k\, t_j$, $dt_j = \sum_{\mu+\nu=j} t_\mu \otimes t_\nu$, $\varepsilon(t_j) = \delta_{0j}$ for $0 \leq i \leq \infty$. (cf. 1.2.6a).

Comment on the proof: it is an easy exercise in Cartierdualisation.

Lemma 2. Let $G \in CAl_k$ and $\phi \in Al_k(G,T_i)$, $0 \leq i \leq \infty$. Then:

a Writing $\phi(g) = \sum_{\mu}^{i} \phi_\mu(g)t^\mu = (\sum_{\mu}^{i} \phi_\mu t^\mu)(g)$ we have: ϕ is determined by $\{\phi_\mu\}_{0\leq\mu\leq i}$ and $\phi_\mu \in \hat{G}$, $0 \leq \mu \leq i$.

b A set $\{\phi_\mu\}_{0\leq\mu\leq i} \subset \hat{G}$ determines $\phi = \sum_{\mu}^{i} \phi_\mu t^\mu \in Al_k(G,T_i)$ iff the ϕ_μ satisfy the Leibnizrelations (1.5) or equivalently the relations (1.6)

$$(1.5) \qquad \phi_\mu(gh) = \sum_{\rho+\sigma=\mu} \phi_\rho(g)\ \phi_\sigma(h) \quad \text{for all } 0 \leq \mu \leq i;\ g,h \in G;$$

$$(1.6) \qquad d\phi_\mu = \sum_{\rho+\sigma=\mu} \phi_\rho \otimes \phi_\sigma \quad \text{for all } 0 \leq \mu \leq i.$$

Proof. a. The only point is continuity. Now $t_n \in T_i^*$ (lemma 1) satisfies: $\langle t_n, t^m\rangle = \delta_{n,m}$. Because ϕ_μ is the composition map $G \xrightarrow{\phi} T_i \xrightarrow{t_\mu} k$ and ϕ, t_μ are continuous, $\phi_\mu \in G^*$.

b. The equivalence of (1.5) and (1.6) is clear from Cartierdualisation. (1.5) is equivalent with the assertion that $\phi(gh) = \phi(g)\phi(h)$ for all $g,h \in G$. Thus suppose: $\{\phi_\mu\}_{0\leq\mu\leq i} \subset G^*$ satisfies the Leibnizrelations, then

$\phi = \sum^{i} \phi_\mu t^\mu$ is obviously a morphism of k-algebras. As for the continuity of ϕ we notice the following:

Let (t^n) be the ideal in T_i, generated by t^n, then

$$\phi^{-1}((t^n)) = \{g \in G \mid \phi(g) = \sum^{i} \phi_\mu(g)t^\mu \in (t^n)\} = \bigcap_{\mu=0}^{n-1} \operatorname{Ker} \phi_\mu.$$

Now $\phi_\mu \in G^*$ and k has discrete topology, so $\operatorname{Ker} \phi_\mu$ is open, hence $\phi^{-1}((t^\mu))$ is open and lemma 2 is proven.

Lemma 3. Let $?^* : \mathrm{Al}_k(G,T_i) \to \mathrm{Coalg}_k(T_i^*,G^*)$ be the canonical map obtained from Cartierdualisation. If $\phi = \sum^{i} \phi_\mu t^\mu \in \mathrm{Al}_k(G,T_i)$, then with the notations of lemma 1, ϕ^* is determined by $\phi^*(t_\mu) = \phi_\mu$, $0 \leq \mu \leq i$. Conversely, if $h \in \mathrm{Coalg}_k(T_i^*,G^*)$ and $h(t_\mu) = h_\mu$, then $\tilde{h} = \sum^{i} h_\mu t^\mu \in \mathrm{Al}_k(G,T_i)$ and $(\tilde{h})^* = h$.

Proof. The first assertion is obvious from the relations

$$\langle \phi^*(t_\mu), g\rangle = \langle t_\mu, \phi(g)\rangle = \langle t_\mu, \sum^{i} \phi_\nu(g)t^\nu\rangle = \langle \phi_\mu, g\rangle \text{ for all } g \in G.$$

If $h(t_\mu) = h_\mu$, then the h_μ must satisfy the relation (1.6), thus define the morphism $\tilde{h} = \sum^{i} h_\mu t^\mu$. $(\tilde{h})^* = h$ is clear.

Lemma 4. Let $G \in \mathrm{CAl}_k$ and $0 \leq i \leq \infty$. Then:

a the natural groupstructure on $\mathrm{Al}_k(G,T_i)$ is given by

$$(\sum^{i} \phi_\mu t^\mu)(\sum^{i} \psi_\nu t^\nu) = \sum_{j=0}^{i} \Big(\sum_{\mu+\nu=j} \phi_\mu \psi_\nu \Big) t^j.$$

The products $\phi_\mu \psi_\nu$ are taken in G^*.

b $\mathrm{Al}_k(G,T_i)$ is the semidirect product of the group

$$\mathrm{Sep}(G) = \{\sum^{i} \phi_\mu t^\mu \in \mathrm{Al}_k(G,T_i) \mid \phi_\mu = 0 \text{ if } \mu > 0\}$$

and the invariant subgroup

$$\mathrm{Inf}_i(G) = \{\sum^{i} \phi_\mu t^\mu \in \mathrm{Al}_k(G,T_i) \mid \phi_0 = \varepsilon : G \to k\}.$$

This decomposition is functorial in $G \in \mathrm{CAl}_k$.

Proof. a. Let $\phi = \Sigma^{i} \phi_\mu t^\mu$ and $\psi = \Sigma^{i} \psi_\mu t^\mu$. By definition of the formal cogroupstructure on G, the product $\phi\psi$ of ϕ and ψ in the group $Al_k(G,T_i)$ is given by the diagram $G \to G \hat{\otimes} G \xrightarrow{\phi \hat{\otimes} \psi} T_i \hat{\otimes} T_i \to T_i$ or equivalently by Cartierdualisation, by the diagram

$$T_i^\times \to T_i^\times \otimes T_i^\times \xrightarrow{\phi^\times \otimes \psi^\times} G^\times \otimes G^\times \xrightarrow{d^\times} G^\times$$

giving $(\phi\psi)^\times$, and $(\phi\psi)^\times(t_j) = d^\times \circ \phi^\times \otimes \psi^\times (\sum_{\mu+\nu=j} t_\mu \otimes t_\nu) =$ lemma 3 $d^\times(\sum_{\mu+\nu=j} \phi_\mu \otimes \psi_\nu) = \sum_{\mu+\nu=j} \phi_\mu \psi_\nu$. Again by lemma 3, a. follows.

b. First notice that Sep(G) and $Inf_i(G)$ are indeed subgroups. The canonical map $T_i \to T_o = k$ induces the grouphomomorphism $\rho_{io} : Al_k(G,T_i) \to Al_k(G,k)$, $\Sigma^{i} \phi_\mu t^\mu \mapsto \phi_o$ which admits the section $\phi_o \mapsto \phi_o + o.t + \ldots + o.t^i$. Thus $Al_k(G,k) \simeq Sep(G)$. Ker $\rho_{io} = \{\Sigma^{i} \phi_\mu t^\mu \mid \phi_o = \varepsilon : G \to k\} = Inf_i(G)$. Functoriality is evident.

Remark 1. It is obvious that this decomposition of $Al_k(G,T_i)$ is closely related with the decomposition of formal groups (i.e. the opposite category of CAl_k) in a semidirect product of an etale and an infinitesimal part if k is perfect. [PGB 2.5.2].

Lemma 5. Let $G \in CAl_k$ and Z(i) as defined in (1.2.9), $0 \leq i \leq \infty$. Then the morphism $h : T_i^\times \to Z(i)$ in $Coalg_k$, defined by $h(t_\mu) = Z_\mu$, $0 \leq \mu \leq i$, induces an injection

$$h^\times : GCoalg_k(Z(i),G^\times) \hookrightarrow Coalg_k(T_i^\times,G^\times)$$

and Im $h^\times$ = image of $Inf_i(G)$ under $?^\times$ (lemma 3 and 4).

Proof. Because every morphism $\phi : Z(i) \to G^\times$ in $GCoalg_k$ is determined by the $\phi(Z_\mu) \in G^\times$, $0 \leq \mu \leq i$, $h^\times$ is injective. Moreover: $\phi(Z_0) = \phi(1) = 1 \in G^\times$, and because $1 \in G^\times$ is the map $\varepsilon : G \to k$, Im $h^\times$ is contained in the image of $Inf_i(G)$. Thus let $\phi = \Sigma^{i} \phi_\mu t^\mu \in Inf_i(G)$, then $\phi^\times \in Coalg_k(T_i^\times,G^\times)$ satisfies

$\phi^*(t_\mu) = \phi_\mu$. Define $\overline{\phi} : Z(i) \to G^\wedge$ as a morphism of k-algebras by $\overline{\phi}(Z_\mu) = \phi_\mu$. $\overline{\phi}$ is a unitary morphism. We are done if $\overline{\phi}$ is a morphism of coalgebras, i.e. $\overline{\phi}$ is compatible with d and ε, but this is easily verified for the generators $Z_\mu \in Z$. Because d and ε are morphisms of k-algebras, it follows that $\overline{\phi} \otimes \overline{\phi} \circ d = d \circ \overline{\phi}$ and $\varepsilon \circ \overline{\phi} = \varepsilon$. Evidently $h^\wedge(\overline{\phi}) = \phi^*$ and we are done.

Lemma 6. a. For $0 \leq i \leq \infty$, $Z(i)$ is a cogroup object in $GCoalg_k$, i.e. $GCoalg_k(Z(i),-)$ is a groupfunctor.

b. If $X \in GCoalg_k$ and $\phi,\psi : Z(i) \rightrightarrows X$ are morphisms in $GCoalg_k$, defined by $\phi(Z_\mu) = \phi_\mu$, $\psi(Z_\mu) = \psi_\mu$, their product $\phi\psi$ in the group $GCoalg_k(Z(i),X)$ is defined by $\phi\psi(Z_\mu) = \sum_{\rho+\sigma=\mu} \phi_\rho \psi_\sigma$, $0 \leq \mu \leq i$.

a By lemma 5 and Cartierduality, $GCoalg_k(Z(i),X) \overset{h^\wedge}{\to}$ image of $Inf_i(X^*)$ under $?^*$, and this is evidently functorial in X, thus, giving $GCoalg_k(Z(i),X)$ the induced groupstructure of $Inf_i(X^*)$, a follows.

b $h^\wedge(\phi)\ (t_\mu) = \phi_\mu$ and $h^\wedge(\psi)\ (t_\mu) = \psi_\mu$. Observing that $h^\wedge(\phi\psi)$ corresponds with the composite map (cf. proof of lemma 4a):

$$h^\wedge(\phi\psi) : T_i^\wedge \to T_i^\wedge \otimes T_i^\wedge \xrightarrow{h^\wedge(\phi) \otimes h^\wedge(\psi)} X \otimes X \to X,$$

one finds easily $h^\wedge(\phi\psi)\ (t_\mu) = \sum_{\rho+\sigma=\mu} \phi_\rho \psi_\sigma$, $0 \leq \mu \leq i$ and then b is evident.

Lemma 7. The map $Al_k(G,T_i) \to G^\wedge[[t]]/(t^{i+1})$, $\phi \mapsto \Sigma\phi_\mu t^\mu$, in the notations of lemma 2, i.e. $\phi(g) = \sum_0^i \phi_\mu(g)t^\mu$ for $g \in G$, factorizes through the multiplicative subgroup of units of $G^\wedge[[t]]/(t^{i+1})$ and is an injective homomorphism of groups.

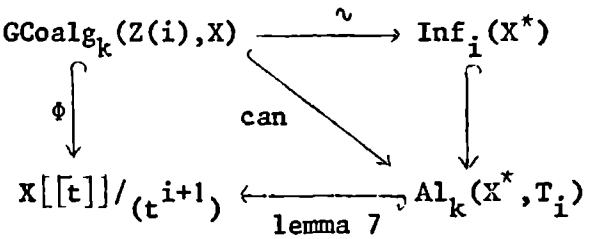
Proof. This is evident from lemma 4a.

Now the diagram $GCoal_k(Z(i),G^*) \overset{h^\wedge}{\hookrightarrow} Coalg_k(T_i^\wedge,G^\wedge) \overset{?^*}{\underset{\sim}{\leftarrow}} Alg_k(G,T_i)$ defines an

embedding $GCoalg_k(Z(i),G^*) \overset{can}{\hookrightarrow} Al_k(G,T_i)$, called canonical and functorial in $G \in CAl_k$. can is by definition a homomorphism of groups, and is a bijection if $G \in ICAl_k$. can is a bijection on the subgroup $Inf_i(G)$, functorial in G. By Cartierduality it amounts to the same to consider can as an embedding of groups, $GCoalg_k(Z(i),X) \overset{can}{\hookrightarrow} Al_k(X^*,T_i)$, functorial in $X \in GCoalg_k$. Summarizing our results we have:

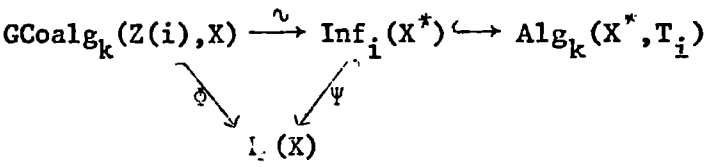
1.4.7. Second embedding diagram.

a There exists a commutative diagram, functorial in $X \in GCoalg_k$, $0 \leq i \leq \infty$,



where Φ is defined by the other arrows, factorizing through the multiplicative subgroup of $X[[t]]/(t^{i+1})$, $0 \leq i \leq \infty$.

Let $H_i(X) \underset{\text{def}}{=} \text{Im } \Phi$, endowed with the natural groupstructure, then in the commutative diagram



all morphisms are morphisms of groups, functorial in X. Ψ is induced by the other arrows.

b Let $\phi = \sum_{\mu}^{i} \phi_\mu t^\mu \in H_i(X)$, then denoting Φ^{-1} and Ψ^{-1} the inverses of Φ and Ψ, we have

$\{\Phi^{-1}(\phi)\}(Z_\mu) = \phi_\mu$ and $\{\Psi^{-1}(\phi)\}(g) = \sum_{\mu}^{i} \phi_\mu(g) t^\mu$ for $g \in X^*$, $0 \leq \mu \leq i$.

From now on we shall identify the elements of $GCoalg_k(Z(i),X)$ and $Inf_i(X^*)$ with their images in $H_i(X)$, and thus $\phi = \sum_{\mu}^{i} \phi_\mu t^\mu \in H_i(X)$ means:

$\phi(Z_\mu) = \phi_\mu$ if ϕ is considered as an element of $GCoalg_k(Z(i),X)$.

$\phi(g) = \sum^{i} \phi_\mu(g)t^\mu$ if ϕ is considered as an element of $Inf_i(X^*)$. $(g \in X^*)$.

c The groupstructure on the sets $GCoalg_k(Z(i),X)$, $Inf_i(X^*)$ and $H_i(G)$ is defined by the relations: If $\phi = \sum^{i} \phi_\mu t^\mu$ and $\psi = \sum^{i} \psi_\mu t^\mu$ then

$$\phi\psi = (\sum^{i} \phi_\mu t^\mu)(\sum^{i} \psi_\nu t^\nu) = \sum_{j=0}^{i} \Big(\sum_{\mu+\nu=j} \phi_\mu \psi_\nu \Big) t^j$$ (cf. lemma 4a and 6b).

1.4.8. Definition. Let $G \in GCoalg_k$ and $0 \leq i \leq \infty$. An element of $H_i(G)$ will be called a curve of order i in G. By (1.4.7b) we may as well consider curves of order i in G to be elements of $GCoalg_k(Z(i),G)$ or $Inf_i(G^*)$. The particular curve $\sum^{i} Z_\mu t^\mu$ in $H_i(Z(i))$, corresponding with the identity map on Z(i) is called the canonical curve of order i, and if $i = \infty$, $\Sigma Z_\mu t^\mu$ will be called the canonical curve. The set of curves of order i in G form a group, functorial in G (1.4.7c). Notice that if G is abelian and if G^* is a Dieudonné formal cogroup (1.1.10a), a curve of order ∞ in G, shortly a curve in G is essentially the same as a curve in the sense of P. Cartier [9§2]. We shall write H(G) instead of $H_\infty(G)$.

1.4.9. Algebraic properties of $H_i(G)$, $0 \leq i \leq \infty$. Then:

Lemma. Let $G \in GCoalg_k$ and $0 \leq i \leq \infty$.

a For every $n > 0$, $V_n : H_i(G) \to H_{in}(G)$, $V_n(\sum^{i} \phi_\mu t^\mu) = \sum^{in} \phi_\mu t^{n\mu}$ is an injective homomorphism of groups, functorial in G.

b For $0 \leq j \leq i \leq \infty$, $\rho_{ji} : H_i(G) \to H_j(G)$, $\rho_{ji}(\sum^{i} \phi_\mu t^\mu) = \sum^{j} \phi_\mu t^\mu$ is a homomorphism of groups, functorial in G.

c For every $\lambda \in k$, $\lambda* : H_i(G) \to H_i(G)$, $\lambda*(\sum^{i} \phi_\mu t^\mu) = \sum^{i} \lambda^\mu \phi_\mu t^\mu$ defines an operation of k on $H_i(G)$, satisfying:

$\lambda*(\mu* \phi) = (\lambda\mu)* \phi$, $\lambda* (\phi\psi) = (\lambda* \phi).(\lambda* \psi)$, $1* \phi = \phi$, $0* \phi = 1$.

The operation is functorial in G.

1.4.10. Topological properties of the $H_i(G)$, $0 \leq i \leq \infty$:

a The (t)-adic topology on $G[[t]]/(t^{i+1})$ induces on $H_i(G)$ the structure of topological group. The topology is discrete if $i < \infty$, and $H(G)$ is a complete separated topological group.

b $T = \varprojlim T_i$ in Al_k induces $H(G) = \varprojlim H_i(G)$, and thus $H(G)$ bears a natural structure of complete separated topological group in the $\varprojlim$-topology.

c The topologies, defined in a and b on $H(G)$ coincide and the invariant subgroups

$$\{H(G)\}_n = \{\Sigma\phi_\mu t^\mu \in H(G) \mid \phi_1 = \ldots = \phi_n = 0\}$$

constitute a fundamental system of neighborhoods of the neutral element 1 in $H(G)$.

d If $\phi : G \to G_1$ is a morphism in $GCoalg_k$, then the induced homomorphism $H(\phi) : H(G) \to H(G_1)$ is continuous.

Proof. Observe that the $\{H(G)\}_n$ is a fundamental system of neighborhoods of $1 \in H(G)$ in the topology of a, and that $\{H(G)\}_n$ is the kernel of the canonical map $H(G) \to H_n(G)$. Because the $\varprojlim$-topology defines a complete separated topology, a, b and c are clear. The continuity of $H(\phi)$ is trivial.

1.4.11. Remark. (1.4.10) ensures the possibility to deal with denumerably infinite products of curves in G. One only has to verify that the product converges in the (t)-adic topology on $H(G)$. Because the group $H(G)$ is in general not commutative, we define for $w_i \in H(G)$, $i \geq 1$, $\prod_{i=1}^{n} w_i$ recurrently by $\prod_{i=1}^{n+1} w_i = (\prod_{i=1}^{n} w_i)w_{n+1}$, $\prod_{i=1}^{1} w_i = w_1$ and $\prod_{i=1}^{\infty} w_i = \lim_{n\to\infty} \prod_{i=1}^{n} w_i$. One then has: the product $\prod_{i=1}^{\infty} w_i$ converges iff the w_i converge to the neutral element $1 \in H(G)$, as is clear from the topology on $H(G)$. For the algebraic and topological properties in the abelian case, compare [9, §2].

§5 Properties of the Verschiebung V.

Let k again be a field, $\chi(k) = p > 0$.

We do not assume that k is perfect. $G \in GCoalg_k$ will be an arbitrary object. If $A \in Al_k$, we put $F^iA = \{a^{p^i} \in A \mid a \in A\}$ and $F^ia = a^{p^i}$.

1.5.1. Let $g \in G$ be such that $\langle g, x^p \rangle \in Fk$ for every $x \in G^*$. In view of the unicity of p^{th}-roots, we then may define Vg by the relation: $\langle Vg, x \rangle = \langle g, Fx \rangle^{1/p}$. Notice that $Vg \in G$. Indeed: Vg is k-linear and for the continuity of Vg we remark that there exists an open ideal of finite colength $\mathcal{a} \subset G^*$, such that $\langle g, \mathcal{a} \rangle = 0$. Now if $a \in \mathcal{a}$, $\langle Vg, a \rangle = \langle g, Fa \rangle^{1/p} = 0$ because $Fa \in \mathcal{a}$, thus Vg is continuous. We say in this case: Vg is defined.

1.5.2. The following two lemmata show the analogy between F and V.

Lemma 1. Let $F : G^* \to G^*$ be the Frobenius map $x \mapsto x^p$, then

a $F(f+g) = Ff + Fg$, $F(fg) = Ff.Fg$, $F(\lambda f) = \lambda^p Ff$ if $g,f \in G^*$, $\lambda \in k$.

b $F \otimes F \circ d = d \circ F$, $F \circ \varepsilon = \varepsilon \circ F$, denoting $\lambda \mapsto \lambda^p$ on k again by F.

Lemma 2. If k is perfect, $V : G \to G$ is defined and

a $V(g+h) = Vg + Vh$, $V(gh) = Vg.Vh$, $V(\lambda^p g) = (\lambda V)(g)$ if $g,f \in G$, $\lambda \in k$.

b $V \otimes V \circ d = d \circ V$, $V \circ \varepsilon = \varepsilon \circ V$, denoting $\lambda \mapsto \lambda^{1/p}$ on k again by V.

The verifications of lemma 2 are all easy, e.g. $\langle V \otimes V \circ dg, x \hat{\otimes} y \rangle = \langle V \otimes V (\Sigma g_i \otimes g_i'), x \hat{\otimes} y \rangle = \Sigma \langle Vg_i, x \rangle \langle Vg_i', y \rangle = (\Sigma \langle g_i, Fx \rangle \langle g_i', Fy \rangle)^{1/p} = \langle dg, Fx \hat{\otimes} Fy \rangle^{1/p} = \langle g, F(xy) \rangle^{1/p} = \langle Vg, xy \rangle = \langle dVg, x \hat{\otimes} y \rangle$. Here we have put $dg = \Sigma g_i \otimes g_i'$. $\langle \varepsilon \circ V(g), \lambda \rangle = \langle Vg, \eta(\lambda) \rangle = \langle g, \eta(F\lambda) \rangle^{1/p} = \langle \varepsilon(g), F\lambda \rangle^{1/p} = \langle V\varepsilon(g), \lambda \rangle$. If k is not perfect, then lemma 2 a is true if Vg and Vh are defined and lemma 2b is true if Vg_i, Vg_i' and Vg are defined.

1.5.3. Lemma. Let $\phi = \Sigma^i \phi_\mu t^\mu$ be a curve in G, $0 \leq i \leq \infty$. Then $V\phi_\mu$ is defined for every μ and $V\phi_\mu = 0$ if $(\mu,p) = 1$ and $V\phi_{p\mu} = \phi_\mu$ for all μ.

Proof. Consider by the second embedding diagram (1.4.7b) ϕ as an element of $Al_k(G^\times,T_i)$. Then $\phi(a^p) = \phi(a)^p$ gives: $\Sigma\phi_\mu(a^p)t^\mu = \Sigma\phi_\mu(a)^p t^{p\mu}$, i.e.: $\phi_\mu(a^p) = 0$ if $(\mu,p) = 1$ and $\phi_{\mu p}(a^p) = \phi_\mu(a)^p$, i.e. $\phi_\mu(FG^\times) \subset k^p$, thus $V\phi_\mu$ is defined. The remaining assertions now are evident.

Corollary. Let Z be the UNG_k, then VZ_μ is defined and $VZ_\mu = 0$ if $(\mu,p) = 1$, $VZ_{\mu p} = Z_\mu$ for all μ.

Indeed: apply the lemma to the canonical curve $\Sigma Z_\mu t^\mu$.

The following three lemmata give the compatibility of V, curves and the first embedding diagram (1.4.5).

1.5.4. Lemma. Let $x = \overset{i}{\Sigma} x_\mu t^\mu$ be a curve in G, $0 \leq i \leq \infty$. With the notations of (1.4.5), i.e. $\mu : G \to Lin_k(G^\times,G^\times)$, $\mu(x_\nu) = \bar{x}_\nu$, we have:

$$\bar{x}_n(gh) = \sum_{\mu+\nu=n} \bar{x}_\mu(g)\,\bar{x}_\nu(h) \quad \text{for all } g,h \in G', \ 0 \leq n \leq i.$$

In particular: $\bar{x}_0$ is the identity map on G^* and $\bar{x}_1$ is a continuous k-derivation on G^*.

Proof. Write $dg = \sum_{i \in S} g_i \hat{\otimes} g_i'$, $dh = \sum_{i \in S} h_i \hat{\otimes} h_i'$ for a suitable index set S. Then:

$$\begin{aligned}
\bar{x}_n(gh) &= 1 \hat{\otimes} x_n(d(gh)) = 1 \hat{\otimes} x_n\Big(\sum_{i,j \in S} g_i h_j \hat{\otimes} g_i' h_j'\Big) \\
&= \sum_{i,j \in S} g_i h_j \langle x_n, g_i' h_j' \rangle \\
&= \sum_{i,j \in S} \sum_{\mu+\nu=n} g_i h_j \langle x_\mu, g_i' \rangle \langle x_\nu, h_j' \rangle \qquad \text{(Cartierduality)} \\
&= \sum_{\mu+\nu=n} \Big(\sum_{i \in S} g_i \langle x_\mu, g_i' \rangle\Big)\Big(\sum_{j \in S} h_j \langle x_\nu, h_j' \rangle\Big) \qquad (x_\mu, x_\nu \text{ have finite dimensional support}) \\
&= \sum_{\mu+\nu=n} \bar{x}_\mu(g)\,\bar{x}_\nu(h).
\end{aligned}$$

We have $x_0 = 1 \in G$, acting as $\varepsilon : G^* \to k$, thus $\bar{x}_0 = 1 \hat{\otimes} \varepsilon \circ d = id$.

Further $\overline{x}_1(gh) = \overline{x}_1(g)\,\overline{x}_0(h) + \overline{x}_0(g)\,\overline{x}_1(h) = \overline{x}_1(g)h + g\,\overline{x}_1(h)$.

1.5.5. Lemma. Let $x \in G$ and let Vx be defined, then $\overline{x} \circ F = F \circ \overline{Vx}$.

Proof. Let $g \in G^*$, $dg = \sum_{i \in S} g_i \hat{\otimes} g_i'$, then using the fact that F is continuous:

$$\overline{x} \circ F(g) = 1 \hat{\otimes} x \Big(\sum_{i \in S} g_i^p \hat{\otimes} g_i'^p \Big) = \sum_{i \in S} g_i^p \langle x, g_i'^p \rangle =$$

$$= F\Big(\sum_{i \in S} g_i \langle Vx, g_i' \rangle \Big) = F \circ \overline{Vx}(g).$$

1.5.6. Lemma. Let $x = \sum^{i} x_\mu t^\mu$ be a curve in G, $0 \leq i \leq \infty$, then:

a $\overline{x}_\mu$ is F^nG^*-linear for $0 \leq \mu \leq p^n-1$, $n \geq 0$.

b $\overline{x}_{p^n}$ is a F^nk-derivation on F^nG^*, all $n \geq 0$.

Proof. Observe that in view of (1.5.3) Vx_μ is defined for every $\mu \geq 0$ and that V can be considered as an endomorphism of the set $\{x_\mu\}_{\mu \geq 0}$. Thus the r^{th}-iteration V^r is defined for x_μ, and lemma (1.5.5) then gives: $\overline{x}_\mu \circ F^n = F^n \circ \overline{V^n x_\mu}$, thus if $0 \leq \mu \leq p^n-1$:

$$\overline{x}_\mu(a^{p^n}.b) = \sum_{\rho+\sigma=\mu} \overline{x}_\rho(a^{p^n})\,\overline{x}_\sigma(b) \qquad \text{(lemma 1.5.4)}$$

$$= \sum_{\rho+\sigma=\mu} F^n \circ \overline{V^n x_\rho}(a).\overline{x}_\sigma(b) \qquad \text{(lemma 1.5.5)}$$

$$= a^{p^n}.\overline{x}_\mu(b) \qquad (V^n x_\rho = 0 \text{ if } 1 \leq \rho \leq p^n-1,\ Vx_0 = \mathrm{id}).$$

For b observe: $\overline{x}_{p^n}(a^{p^n}b^{p^n}) = F^n \circ \overline{V^n x}_{p^n}(ab)$

$$= F^n \circ \overline{x}_1(ab).$$

Now $\overline{x}_1$ is a k-derivation (1.5.4) on G^* and we are done.

1§6 Technical lemmas.

Preliminary remark: Our aim in this section is to show that if Z is the UNG_k, then $Z^* \underset{\sim}{\sim} k[[X_i]]_{i \geq 1}$ as a k-algebra, (cf. 1.3.8), k being an arbitrary

field, $\chi(k) = p > 0$. There exist two obvious methods in order to arrive at this result. First: A direct proof that the noetherian condition in (1.3.9) is not essential and eliminate the perfectness condition by extension of the base field. The other way is to prove that Z is a hyper-algebra in the sense of Dieudonné-Cartier [4 , page 208], then apply PCL. We will follow however a different way, using ordered p-bases. We recall that $VZ_\mu = 0$ if $(\mu,p) = 1$ and $VZ_{\mu p} = Z_\mu$, $\mu \geq 0$.

1.6.1. In view of the ω-filtration on Z, Z has a denumerable base as a k-vectorspace and thus every linear subspace of Z has a denumerable base.

Lemma. Let $\{p_{oj}\}_{j\geq 1}$ be a denumerable base for $P(Z) \underset{\text{def}}{=} \{z \in Z \mid dz = z \otimes 1 + 1 \otimes z\}$. Define the set $\{p_{ij}\}_{i\geq 0, j\geq 1}$ as follows:

if $p_{oj} = \sum_{(\varepsilon_1,\ldots,\varepsilon_r)} \lambda_{\varepsilon_1,\ldots,\varepsilon_r} Z_{\varepsilon_1}\ldots Z_{\varepsilon_r}$, then

$p_{ij} = \sum_{(\varepsilon_1,\ldots,\varepsilon_r)} \lambda^{p^i}_{\varepsilon_1,\ldots,\varepsilon_r} Z_{p^i\varepsilon_1}\ldots Z_{p^i\varepsilon_r}$. The domain of summation is a finite subset of the set of all ordered finite sequences of natural numbers.

We then have for every $i \geq 0$, $j \geq 1$:

a $Vp_{i,j}$ is defined and $Vp_{i,j} = p_{i-1,j}$. (Put $p_{-1,j} = 0$ for every j).

b $\overline{p_{ij}}$ is $F^{i+1}Z^*$-linear on Z^* and $\overline{p_{ij}} \circ F^i = F^i \circ \overline{p_{oj}}$.

c The restriction of $\overline{p_{ij}}$ to F^iZ^* is a F^ik-derivation on F^iZ^*.

Proof.

a If $i \geq 1$, everything is clear (1.5.3 corollary, 1.5.2). If $i = 0$, then $1 + p_{oj}t$ is a curve of order 1 in Z. By (1.5.3) we then have $Vp_{oj} = 0$.

b Let $u,v \in Z^*$, then:

$$\langle p_{ij}, u^{p^{i+1}} v\rangle = \langle \Sigma\lambda^{p^i}_{\varepsilon_1,\ldots,\varepsilon_r} Z_{\eta_1}\ldots Z_{\eta_r} \otimes Z_{\theta_1}\ldots Z_{\theta_r}, u^{p^{i+1}} \hat{\otimes} v\rangle$$

where the summation is to be extended over all $(\varepsilon_1,\ldots,\varepsilon_r)$ and all non

negative integer solutions of $\eta'_m + \theta'_m = p^i\varepsilon_m$, $1 \leq m \leq r$.

Put $\eta_m = \eta'_m p^{-i}$ and $\theta_m = \theta'_m p^{-i}$. We obtain, using V:

$$(1.7)\quad \langle p_{ij}, u^{p^{i+1}} v\rangle = \Sigma \langle \lambda_{\varepsilon_1 \ldots \varepsilon_r} Z_{\eta_1} \ldots Z_{\eta_r}, u^p\rangle^{p^i} \langle Z_{p^i\theta_1} \ldots Z_{p^i\theta_r}, v\rangle$$

If η_m and θ_m are not integers, then following our conventions $Z_{\eta_m} = 0$ and $Z_{\theta_m} = 0$. Thus, writing $dp_{ij} = \Sigma \lambda^{p^i}_{\alpha\beta} M_\alpha \otimes M_\beta$ as a (unique) finite sum of monomials, we have

$$(1.8)\quad \langle p_{ij}, u^{p^{i+1}} v\rangle = \Sigma \langle \lambda_{\alpha\beta} V^i M_\alpha, u^p\rangle^{p^i} \langle M_\beta, v\rangle.$$

From (1.7) and (1.8) it follows: a term $M_\alpha \otimes M_\beta$ in dp_{ij} can give a non zero contribution in (1.8) only if $V^i M_\alpha \neq 0$ implies $M_\beta \in k[Z_{p^i}, Z_{2p^i}, \ldots]$, i.e.: $V^i M_\beta \neq 0$.

On the other hand we have:

$$dp_{oj} = dV^i p_{ij} = V^i \otimes V^i dp_{ij} = \Sigma\, \lambda_{\alpha\beta} V^i M_\alpha \otimes V^i M_\beta \qquad (1.5.2)$$

$$= p_{oj} \otimes 1 + 1 \otimes p_{oj} \qquad \text{(because } p_{oj} \in P(Z)\text{)}.$$

$$= \Sigma\, \lambda_{\varepsilon_1, \ldots, \varepsilon_r} (Z_{\varepsilon_1} \ldots Z_{\varepsilon_r} \otimes 1 + 1 \otimes Z_{\varepsilon_1} \ldots Z_{\varepsilon_r}).$$

It follows: $V^i M_\alpha = 1$ or $V^i M_\alpha = Z_{\varepsilon_1} \ldots Z_{\varepsilon_r}$ for some index $(\varepsilon_1, \ldots, \varepsilon_r)$. If $V^i M_\alpha = 1$, then necessarily $V^i M_\beta = Z_{\varepsilon'_1} \ldots Z_{\varepsilon'_r}$ for some index $(\varepsilon'_1, \ldots, \varepsilon'_r)$ and if $V^i M_\alpha = Z_{\varepsilon_1} \ldots Z_{\varepsilon_r}$, then necessarily $V^i M_\beta = 1$. (Observe that V^i is defined on all monomials and that the set of monomials is closed under the action of V^i).

Furthermore $V^i M_\alpha = 1$ implies $M_\alpha = 1$ if M_α is a monomial.

It follows from this, that (1.8) reduces to:

$$\langle p_{ij}, u^{p^{i+1}} v\rangle = \langle 1, u^p\rangle^{p^i} \langle p_{ij}, v\rangle + \langle p_{oj}, u^p\rangle^{p^i} \langle 1, v\rangle$$

where in the first term on the right hand side all terms in (1.8) are collected such that $V^i M_\alpha = 1$ and in the second term those which satisfy

$V^i M_\beta = 1$.

Now: $\langle p_{oj}, u^p \rangle = \langle p_{-1,j}, u \rangle^p = 0$, thus in view of $\langle 1, u \rangle = \varepsilon(u)$ we have:

$$(1.9) \qquad \langle p_{ij}, u^{p^{i+1}} v \rangle = \varepsilon(u^{p^{i+1}}) \langle p_{ij}, v \rangle .$$

Now let $du = \sum_{s \in S} u_s \hat{\otimes} u'_s$, $dv = \sum_{t \in S} v_t \hat{\otimes} v'_t$, then

$$\begin{aligned} \overline{p_{ij}}(u^{p^{i+1}} v) &= 1 \otimes p_{ij}\Big(\sum_{s,t \in S} u_s^{p^{i+1}} v_t \hat{\otimes} u_s'^{p^{i+1}} v'_t \Big) \\ &= \sum_{s,t \in S} u_s^{p^{i+1}} v_t \, \varepsilon(u_s'^{p^{i+1}}) \langle p_{ij}, v'_t \rangle \qquad (1.9) \\ &= \sum_{s \in S} u_s^{p^{i+1}} \varepsilon(u_s'^{p^{i+1}}) \cdot \sum_{t \in S} v_t \langle p_{ij}, v'_t \rangle \\ &= u^{p^{i+1}} \overline{p_{ij}}(v) \qquad (1 \hat{\otimes} \varepsilon \circ d = \text{identity}). \end{aligned}$$

There are no topological difficulties because p_{ij} has finite dimensional support.

c $\overline{p_{ij}} \circ F^i = F^i \circ \overline{V^i p_{ij}}$ (iteration of (1.5.5), everything is defined)

$= F^i \circ \overline{p_{oj}}$.

Because $1 + p_{oj} t$ is a curve, $\overline{p_{oj}}$ is a k-derivation on Z^* (1.5.4).

c now follows trivially.

1.6.2. Definition. Let $G \in \mathrm{NAlg}_k$. $\chi(k) = p > 0$. A total ordered set $\{e_i\}_{i \in S} \subset G$ is called an ordered p-base for G if the set of all monomials $\{e_{i_1}^{\alpha_1} e_{i_2}^{\alpha_2} \ldots e_{i_r}^{\alpha_r} \mid i_1 < i_2 < \ldots < i_r,\ 0 \leq \alpha_i < p,\ r \geq 1\}$ is a base for G as a k-vectorspace.

1.6.3. Let $\{p_{ij}\}_{i \geq 0, j \geq 1}$ be the set as in (1.6.1). Define a total ordering $<$ by $p_{ij} < p_{ks}$ if $i > k$, all j,s, and

$p_{ij} < p_{ik}$ if $j > k$, all i.

We claim:

Lemma. The set $\{p_{ij}\}_{i\geq 0, j\geq 1}$ is an ordered p-base for Z.

Proof. We combine the proof of this lemma with another result about Z^*, to be stated in (1.6.4). The proof will be given in (1.6.5).

1.6.4. Let $\{H_n\}_{n\geq 0}$ be the ω-filtration on Z. We choose a base $\{e_i\}_{i\geq 1}$ for Z as a k-vectorspace in the following way: The base $\{p_{oj}\}_{j\geq 1}$ for P(Z) (1.6.1) is a subset of $\{e_i\}_{i\geq 1}$ and each H_n has a base which is a subset of $\{e_i\}_{i\geq 1}$. This is possible, because $P(Z) = \bigcup_n \{P(Z) \cap H_n\}$ and because of the fact that P(Z) has a base constisting of homogeneous elements (we obviously may assume the p_{oj} to be homogeneous). Thus in the diagram

$$\begin{array}{ccc} P(Z) \cap H_n & \subset & H_n \\ \cap & & \cap \\ P(Z) \cap H_{n+1} & \subset & H_{n+1} \end{array}$$

we complete a base of $P(Z) \cap H_n$ to a base of H_n, then taking an independent set of homogeneous elements of weight n+1 we can complete the base for $P(Z) \cap H_n$ to a base for $P(Z) \cap H_{n+1}$. Taking all together we complete it to a base for H_{n+1}.

Now let $\{f_i\}_{i\geq 1}$ be the set of pointdistributions on the base $\{e_i\}_{i\geq 1}$ and let in particular $\{w_j\}_{j\geq 1} \subset \{f_i\}_{i\geq 1}$ be such that $\langle w_j, p_{oi}\rangle = \delta_{ij}$.

Let $B = k[[X_i]]_{i\geq 1} \in Al_k$ with topology defined by: each ideal of finite colength in B is open. We assert:

Lemma. The homomorphism of k-algebras $\psi : B \to Z^*$ defined by $\psi(X_i) = w_i$, $i \geq 1$ is an isomorphism in Al_k.

1.6.5. a: ψ is surjective.

Every finite dimensional subspace of Z is contained in some H_n, i.e. the sequence of ideals $\{H_n^{\perp} = \mathrm{Ker}\,(Z^* \to H_n^*)\}_{n\geq 0}$ is a fundamental system of open

neighborhoods of zero in Z^* and $Z^* = \varprojlim H_n^*$. The induced natural filtration on H_n is clearly exhaustive, thus H_n^* is a local k-algebra. (1.3.5). Another way to see this is: We can find an integer N such that $V^N M = 0$ or 1 for every monomial M in the Z_i, $M \in H_n$. Then if $u \in m_n = \mathrm{Ker}\{H_n^* \to H_o^* \tilde{-} k\}$ we have $\langle M, u^{p^N} \rangle = \langle V^N M, u \rangle^{p^N} = 0$ for every monomial $M \in H_n$, thus m_n is a nilpotent ideal. It thus follows that H_n^* is generated as a k-algebra by every set $\{s_j\} \in m_n$ such that the classes $s_j \bmod m_n^2$ generate m_n/m_n^2 as a k-vectorspace. Furthermore:

$$(m_n/m_n^2) = \{f \in H_n^* \mid f(xy) = \varepsilon(x)f(y) + f(x)\varepsilon(y),\ \varepsilon : H_n^* \to H_o^* \tilde{-} k\}$$

$$= \{f \in H_n \mid df = f \otimes 1 + 1 \otimes f\}$$

$$= P(Z) \cap H_n.$$

Because the $\{p_{oj}\}_{j \geq 1}$ is a base for P(Z) and $\{w_j\}_{j \geq 1}$ is the set of point-distributions on this base, the images of the w_j in H_n^* generate H_n^* over k as a k-algebra for every $n \geq 0$. In view of $Z^* = \varprojlim H_n^*$ we conclude: every element in Z^* may be written as a formal powerseries in the w_j, i.e.: ψ is surjective. Let $\mathcal{A}$ be an open ideal in Z^*, thus having finite colength, then $\psi^{-1}(\mathcal{A})$ has finite colength, thus is open in B, so ψ is continuous.

b: ψ is injective.

Let the ordered set $\{p_{ij}\}_{i \geq 0, j \geq 1}$ be chosen as in (1.6.1), (1.6.3). Let T be the indexset of all monomials in the X_i, $X_i \in B$. The corresponding set of monomials will be denoted by $S = \{X^\alpha\}_{\alpha \in T}$. T can be seen as the set of infinite sequences $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_i \ldots)$ of nonnegative integers such that $\alpha_i = 0$ if i is great enough. α then corresponds with the monomial $X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_i^{\alpha_i} \ldots$. T is an additive abelian ordered monoid with zero element $0 \in T$, defined by $X^{\alpha+\beta} = X^\alpha X^\beta$ and $\alpha \leq \beta$ if $X^\alpha X^\gamma = X^\beta$ for some $\gamma \in T$.

We construct a map $D : S \to Z$ as follows:

Consider first the special monomial X_i^{α} and let $\alpha = \sum_0^r \alpha_j p^j$ be the p-adic development of α, then

$$(1.10) \qquad D(X_i^{\alpha}) \underset{\text{Def}}{=} \frac{p_{r,i}^{\alpha_r} \cdot p_{r-1,i}^{\alpha_{r-1}} \cdots p_{0,i}^{\alpha_0}}{\alpha_r! \cdot \alpha_{r-1}! \cdots \alpha_0!} \quad \text{(put } z^0 = 1 \text{ for every } z \in Z\text{)}.$$

Let now $X^{\alpha} = X_1^{\alpha_1} \ldots X_s^{\alpha_s}$ and consider $E(X^{\alpha}) = \prod_{j=1}^{s} D(X_j^{\alpha_j})$.
Clearly: the factors p_{ij}^m occurring in $E(X^{\alpha})$ can be rearranged in one and only one way, giving $D(X^{\alpha})$, such that the factors p_{ij}^m are ordered (as defined in (1.6.3)). This defines $D(X^{\alpha})$ for $\alpha \in T$.

Now consider a special case: $w_j^{\beta} \in Z^*$ and X_i^{α} with p-adic developments $\sum_0^r \beta_j p^j$ and $\sum_0^r \alpha_j p^j$. Then:

$$\langle D(X_i^{\alpha}), w_j^{\beta} \rangle = \langle \frac{p_{r,i}^{\alpha_r} \cdots p_{0,i}^{\alpha_0}}{\alpha_r! \cdots \alpha_0!}, w_j^{\beta_r p^r} \cdots w_j^{\beta_0 p^0} \rangle$$

$$= \varepsilon\{\frac{\bar{p}_{r,i}^{\alpha_r} \cdots \bar{p}_{0,i}^{\alpha_0}}{\alpha_r! \cdots \alpha_0!}, (F^r(w_j^{\beta_r})) \ldots (F^0(w_j^{\beta_0}))\} \qquad \text{((1.4.5) and the formula } \langle p,w \rangle = \varepsilon(\bar{p}(w)).)$$

$$= \varepsilon\{\frac{\bar{p}_{r,i}^{\alpha_r}}{\alpha_r!}(F^r(w_j^{\beta_r})) \ldots \frac{\bar{p}_{0,i}^{\alpha_0}}{\alpha_0!}(F^0(w_j^{\beta_0}))\} \qquad (1.6.1,b)$$

$$(1.11) \qquad = \varepsilon\{(\frac{\bar{p}_{0,i}^{\alpha_n}}{\alpha_r!}(w_j^{\beta_r}))^{p^n} \ldots (\frac{\bar{p}_{0,i}^{\alpha_0}}{\alpha_0!}(w_j^{\beta_0}))^{p^0}\} \qquad (1.6.1,b)$$

It follows: everything is reduced to a computation of derivations, and this is easy in view of the Leibnizrelations:

$$(1.12) \qquad \frac{\partial_1^{s_1} \ldots \partial_r^{s_r}}{s_1! \ldots s_r!}(uv) = \sum_{\substack{\alpha_i + \beta_i = s_i \\ 1 \le i \le r}} \frac{\partial_1^{\alpha_1} \ldots \partial_r^{\alpha_r}}{\alpha_1! \ldots \alpha_r!}(u) \, \frac{\partial_1^{\beta_1} \ldots \partial_r^{\beta_r}}{\beta_1! \ldots \beta_r!}(v).$$

In view of $\langle p_{oi}, w_j \rangle = \delta_{ij}$, (1.10) reduces to:

$$\langle D(X_i^{\alpha}), w_j^{\beta} \rangle = \delta_{ij}\, \delta_{\alpha_r,\beta_r} \cdots \delta_{\alpha_0,\beta_0} = \delta_{ij}\, \delta_{\alpha,\beta}.$$

Let now X^{α} and $w^{\beta} = w_1^{\beta_1} \ldots w_m^{\beta_m}$ be arbitrary. Adding eventually exponents $= 0$, we may write $X^{\alpha} = X_1^{\alpha_1} \ldots X_m^{\alpha_m}$. Let $\alpha_k = \sum_{j=0}^{r} \alpha_{kj} p^j$ and $\beta_k = \sum_{j=0}^{r} \beta_{kj} p^j$ be the p-adic developments, $1 \leq k \leq m$. In view of the foregoing

$$\langle D(X^{\alpha}), w^{\beta} \rangle = \prod_{\rho=0}^{r} f_{\rho}, \text{ where} \tag{1.13}$$

$$f_{\rho} = \varepsilon\{\frac{\overline{p}_{0,m}^{\alpha_{m,\rho}}\, \overline{p}_{0,m-1}^{\alpha_{m-1,\rho}} \cdots \overline{p}_{0,1}^{\alpha_{1,\rho}}}{\alpha_{m,\rho}!\, \alpha_{m-1,\rho}! \cdots \alpha_{1,\rho}!} (w_m^{\beta_{m,\rho}} \ldots w_1^{\beta_{1,\rho}})\}^{p^{\rho}}$$

$$= \varepsilon\{\frac{\overline{p}^{\underline{\alpha}}}{\underline{\alpha}!}(w^{\underline{\beta}})\}^{p^{\rho}} \quad \text{using a known shorthand notation.}$$

Using (1.12) and the monoid structure on the vectors $\underline{\alpha}$, we have:

$$f_{\rho} = \sum_{\underline{\alpha}_1 + \underline{\alpha}_2 = \underline{\alpha}} \varepsilon\{\frac{\overline{p}^{\underline{\alpha}_1}}{\underline{\alpha}_1!}(w^{\underline{\beta}_1})\, \frac{\overline{p}^{\underline{\alpha}_2}}{\underline{\alpha}_2!}(w^{\underline{\beta}_2})\}$$

where $\underline{\beta}_1 + \underline{\beta}_2 = \underline{\beta}$ is any decomposition of $\underline{\beta}$.

Put for any vector $(\gamma_1, \ldots, \gamma_m) = \underline{\gamma}$, $|\underline{\gamma}| = \Sigma \gamma_i$. We claim:

1 $|\underline{\beta}| > |\underline{\alpha}|$ implies $f_{\rho} = 0$

2 $|\underline{\beta}| = |\underline{\alpha}|$ implies $f_{\rho} = \delta_{\underline{\alpha},\underline{\beta}}$.

We proceed by induction with respect to $n = |\underline{\beta}|$. If $n = 0$ we have $w^{\beta} = 1$ and the assertion is evidently true. So let $n \geq 0$ and assume 1 and 2 to be true if $|\beta| < n$.

Choose a decomposition $\underline{\beta} = \underline{\beta}_1 + \underline{\beta}_2$. If $|\underline{\beta}| > |\underline{\alpha}|$ then $|\underline{\beta}_1| > |\underline{\alpha}_1|$ or $|\underline{\beta}_2| > |\underline{\alpha}_2|$ in view of $|\underline{\alpha}_1 + \underline{\alpha}_2| = |\underline{\alpha}_1| + |\underline{\alpha}_2|$ and the inductionhypothesis works. If $|\underline{\beta}| = |\underline{\alpha}|$ then we always have $|\underline{\beta}_1| > |\underline{\alpha}_1|$ or $|\underline{\beta}_2| > |\underline{\alpha}_2|$ unless $|\underline{\alpha}_1| = |\underline{\beta}_1|$ and $|\underline{\alpha}_2| = |\underline{\beta}_2|$ and the induction hypothesis works again, giving in this case:

$$f_{\rho} = \sum_{\underline{\alpha}_1 + \underline{\alpha}_2 = \underline{\alpha}} \delta_{\underline{\alpha}_1,\underline{\beta}_1}\, \delta_{\underline{\alpha}_2,\underline{\beta}_2} = \delta_{\underline{\alpha},\underline{\beta}}.$$

Applying this to (1.13) we now find easily:

$$\langle D(X^{\alpha}), w^{\beta}\rangle = 0 \quad \text{if } \Sigma\alpha_i < \Sigma\beta_i$$

$$= \delta_{\alpha,\beta} \text{ if } \Sigma\alpha_i = \Sigma\beta_i.$$

The injectivity of ψ is now clear: Let $0 = \sum_{\alpha \in T} \lambda_\alpha w^\alpha$, $\lambda_\alpha \in k$ and let $|\alpha_0|$ be minimal, $\lambda_{\alpha_0} \neq 0$. Then: $0 = \langle D(X^{\alpha_0}), \sum_\alpha \lambda_\alpha w^\alpha\rangle = \lambda_{\alpha_0}$, a contradiction.

Because ψ is bijective and every ideal in Z^* of finite colength is open, ψ is an isomorphism in Al_k. It follows immediately from the proof that the set $\{D(X^\alpha)\}_{\alpha \in T}$ is a base for the k-vectorspace Z, thus the set $\{p_{ij}\}_{i\geq 0, j\geq 1}$ is an ordered p-base for Z.
The lemmata (1.6.3) and (1.6.4) are now proven.

1.6.6. For future reference we state the corollaries:

Corollary 1. Let $A \in CAl_k$, such that $A \tilde{=} k[[X_i]]_{i \in S}/\mathcal{A}$, where S is an ordered set and $\mathcal{A}$ is an ideal, generated by $F^{N(i)}X_i$, $1 \leq N(i) \leq \infty$, $i \in S$. (We use the convention that $k[[X]]/(F^\infty X) \tilde{=} k[[X]]$).
Let $\{q_{ij}\}$ be the subset of the pointdistributions on the monomials in the X_i in A, satisfying $\langle q_{ij}, X_j^{pi}\rangle = 1$. Then the set $\{q_{ij} \mid j \in S, 0 \leq i < N(j)\}$ defines an ordered p-base for A^*.

Proof. Define the curves $\psi_j : A \to k[[t]]/(F^{N(j)}t)$ by $\psi_j(X_i) = \delta_{ij}t$. Writing $\psi_j = \Sigma\psi_{j\mu}t^\mu$ it follows that $\psi_{jp^i} = q_{ij}$. Comparing (1.5.3) and (1.5.6) with (1.6.1), the q_{ij} satisfy the same formal properties as the p_{ij}, and we can use the reasoning of (1.6.5) again. The corollary then follows easily.

Corollary 2. Let Z be the UNG_k and let $\{q_{ij} \mid i \geq 0, j \geq 1\} \subset Z$ such that

a $\{q_{oj}\}_{j\geq 1}$ is a base for P(Z),

b $\overline{q}_{ij}$ is $F^{i+1}Z$-linear on Z^*,

c the $\overline{q}_{ij}$ are $F^i k$-derivations on $F^i Z^*$,

then the set $\{q_{ij}\}$ is an ordered p-base for Z.

Proof. Obvious: the conditions a, b and c are the only formal properties of the set $\{p_{ij}\}$ necessary for the proof of lemma (1.6.3).

1.6.7. For future reference we add the following two lemmata:

Lemma. Let $\partial \in P(Z)$, then there exists a curve $\gamma(t) \in H(Z)$ such that $\gamma(t) \equiv 1 + \partial t \pmod{t^2}$.

Proof. As in (1.6.6) define $\psi_j : Z^* \to k[[t]]$ by $\psi_j(w_i) = \delta_{ij}t$. This is well defined in view of lemma (1.6.4). Let $\psi_j = \Sigma\psi_{j\mu}t^\mu$, then it is clear that $\psi_{j1} = p_{oj}$ for every $j \geq 1$.
Because $\{p_{oj}\}_{j\geq 1}$ is a base for P(Z), we have $\partial = \sum_1^n \lambda_i p_{oi}$, $\lambda_i \in k$. With the notations of (1.4.9c) we have, taking the product in the natural order, defined by i:

$$\gamma(t) \underset{\text{Def}}{=} \prod_{i=1}^{n} (\lambda_i * \psi_i) = (1+\lambda_1 p_{o1}t+\ldots)(1+\lambda_2 p_{o2}t+\ldots)\ldots(1+\lambda_n p_{on}t+\ldots)$$

$$\equiv 1 + (\Sigma\lambda_i p_{oi})t \pmod{t^2}$$

$$\equiv 1 + \partial t \pmod{t^2}$$

1.6.8. Lemma. If $\partial \in P(Z)$ and ∂ is isobaric of weight s, then there exists a curve $\gamma \in H(Z)$, $\gamma = \Sigma\gamma_\mu t^\mu$, such that γ_μ is isobaric of weight μ, $\gamma \equiv 1 + \partial t^s \pmod{t^{s+1}}$ and $\gamma_\mu = 0$ if μ is not a multiple of s.

Proof. Fix an integer $n \geq 1$ and suppose that we already have a curve $\gamma_n(t)$ in H(Z), $\gamma_n(t) = \Sigma\psi_\mu t^\mu$ such that $\psi_1 = \partial$ and ψ_μ is isobaric of weight μs for all $0 \leq \mu < n$. Write $\psi_n = \psi_n' + \psi_n''$ where ψ_n' is the isobaric part of ψ_n of weight ns. We claim $\psi_n'' \in P(Z)$. Indeed: d is compatible with the weight function ω, thus

$$d\psi_n'' - \psi_n'' \otimes 1 - 1 \otimes \psi_n'' = \psi_n' \otimes 1 + 1 \otimes \psi_n' - d\psi_n' + \sum_{\substack{\rho+\sigma=n \\ \rho,\sigma\neq n}} \psi_\rho \otimes \psi_\sigma$$

the right hand side is isobaric of weight ns. No monomial in the left hand side has weight ns, thus the left hand side equals zero. In view of (1.6.7), H(Z) contains a curve $\delta_n(t) \equiv 1 - \psi_n''t \pmod{t^2}$, thus with (1.4.9c): $V_n\delta_n(t) \equiv 1 - \psi_n''t^n \pmod{t^{n+1}}$.

Put $\gamma_{n+1}(t) = \gamma_n(t).V_n\delta_n(t) \equiv 1 + \psi_1 t + \ldots + \psi_{n-1}t^{n-1} + \psi_n't^n \pmod{t^{n+1}}$. The sequence $\{\gamma_n(t)\}_{n\geq 1}$ converges to a limit curve $\bar{\gamma}(t)$ because H(Z) is a complete topological group (1.4.10). We have $\gamma = V_s\bar{\gamma}(t) \equiv 1 + \psi_1 t^s \pmod{t^{s+1}} \equiv 1 + \partial t^s \pmod{t^{s+1}}$. Observe that if $\gamma = \Sigma\gamma_\mu t^\mu$, every γ_μ is isobaric of weight μ, and $\gamma_\mu = 0$ if μ is not a multiple of s.

CHAPTER II

Existence of the E_μ-polynomials over the prime field

2§1 Statement of the problem.

2.1.1. Let $G \in ICAl_k$. We recall that the infinitesimal group of G, $Inf_\infty(G) = Inf(G) = Al_k(G,k[[t]])$ can be identified canonically with the group of curves in G^*, $H(G^*) = GCoalg_k(Z,G^*)$, where Z is the UNG_k and G^* is the Cartierdual of G. (1.4.7). In view of Cartierduality the study of infinitesimal groups is equivalent to the study of the groups H(G') where $G' \in GCoalg_k$. From a functorial point of view this study can be reduced to the study of H(Z) itself in view of the simple lemma:

Lemma. Let $\phi = \Sigma\phi_\mu t^\mu$ be any curve in $G \in GCoalg_k$, then ϕ induces a continuous homomorphism of groups $H(\phi) : H(Z) \to H(G)$, $H(\phi)(\Sigma Z_\mu t^\mu) = \phi$.

Proof. Evident. The functor $H : GCoalg_k \to Groups$, defined by $H(G) = Inf(G^*) \subset Al_k(G^*,k[[t]])$ is representable by the pair $(Z, \Sigma Z_\mu t^\mu)$.

By the lemma we conclude: because every curve is image of the canonical curve, we can study the functorial properties of curves by studying the canonical curve $\Sigma Z_\mu t^\mu$.

2.1.2. Let now $k = Q$ be the field of rational numbers, then one observes that H(Z) contains the curve $\exp(Z_1 t) = \Sigma \frac{Z_1^\mu}{\mu!} t^\mu$.

Indeed: in view of (1.4.7) we have: $\phi = \Sigma\phi_\mu t^\mu$ is a curve iff $\phi_0 = 1$ and $d\phi_\mu = \sum_{\rho+\sigma=\mu} \phi_\rho \otimes \phi_\sigma$, $\mu \geq 0$. By the binomium of Newton we have $d(\frac{Z_1^\mu}{\mu!}) = \frac{1}{\mu!}(Z_1 \otimes 1 + 1 \otimes Z_1)^\mu = \sum_{\rho+\sigma=\mu} \frac{Z_1^\rho}{\rho!} \otimes \frac{Z_1^\sigma}{\sigma!}$ thus $\exp Z_1 t$ is a curve in Z. Viewing $\exp Z_1 t$ as an endomorphism of Z, we have: $\mathrm{Im} \exp Z_1 t = Q[Z_1]$ bears a natural induced groupcoalgebra structure, in fact, it is isomorphic with the bialgebra of the additive group. Notice that $Q[Z_1]$ appears as a smallest

non trivial subgroupcoalgebra of Z.

2.1.3. The analoguous problem that now arises if $\chi(k) = p > 0$ is somewhat more difficult to solve in view of:

Lemma. Let $\chi(k) = p > 0$ and $\phi = \Sigma\phi_\mu t^\mu$ be a curve in Z, $\phi_1 \neq 0$. Then $\mathrm{Im}\,\phi = k[\phi_1,\phi_2,\ldots]$ cannot be generated by a finite number of the ϕ_μ.

Proof. By (1.4.7) we consider $\phi : Z^* \to k[[t]]$ as a morphism in Al_k. Because $\phi_1 \neq 0$, there exists $x \in Z^*$, $\langle\phi_1,x\rangle = 1$. By (1.5.6) the $\overline{\phi}_{p^\mu}$ are $F^\mu k$-derivations on $F^\mu Z^*$ and $\overline{\phi}_{p^\mu}(x^{p^\mu}) = \overline{\phi}_{p^\mu} \circ F^\mu(x) = F^\mu \circ V^\mu\phi_{p^\mu}(x) = F^\mu\{\overline{\phi}_1(x)\} \neq 0$, because $\phi_1(x) = \varepsilon \circ \overline{\phi}_1(x) \neq 0$. (We used (1.5.5)). Thus $\overline{\phi}_{p^\mu}$ is not trivial on $F^\mu Z^*$ whereas all $\overline{\phi}_n$, $1 \leq n \leq p^\mu - 1$ are trivial on $F^\mu Z^*$. Using $\varepsilon \circ \overline{\phi}_n = \phi_n$, we finally conclude: $\phi_{p^\mu} \notin k[\phi_1,\ldots,\phi_{p^\mu-1}]$ and the lemma is proven.

From (2.1.3) it follows that if curves $\phi = \Sigma\phi_\mu t^\mu$, $\phi_1 \neq 0$ exist such that $\mathrm{Im}\,\phi = k[\phi_1,\phi_p,\ldots,\phi_{p^i},\ldots]$, then $\mathrm{Im}\,\phi$ is generated over k by a minimal set: every strict subset generates a strict subalgebra. That such curves exist is shown in (2.1.4).

2.1.4. Theorem. (Existence theorem). Let $k = \mathbb{F}_p$ and let Z be the UNG_k. Then:

a There exists a set $\{X_i\}_{i\geq 0} \subset Z$, $X_i = Z_{p^i} + u_i(Z_1,\ldots,Z_{p^{i-1}})$ and X_i is isobaric of weight p^i in $Z_1,\ldots,Z_{p^i}$ for all $i \geq 0$.

b There exists a set $\{E_\mu\}_{\mu\geq 0} \subset k\langle X_0,X_1,\ldots\rangle \subset Z$. E_μ is isobaric of weight μ, $E_0 = 1$, $E_{p^i} = X_i$ for all $\mu \geq 0$, $i \geq 0$.

c $E(t) = \Sigma E_\mu t^\mu$ is a curve in Z.

Corollary. If k is an arbitrary field, $\chi(k) = p > 0$, then with the notations of the theorem, $Z \subset k \otimes_{\mathbb{F}_p} Z$ in a canonical way, and thus E(t) can be viewed as a curve in $k \otimes_{\mathbb{F}_p} Z$, the UNG over k.

The proof will be given in 2§2 and 2§3. Notice that there are no unicity statements made about the u_i and the E_μ. It will appear however that Im E(t) is unique up to isomorphism: cf. 3§1. Notice that it follows from a) that the X_i generate a free subalgebra of Z.

2§2 Proof of the existence theorem over an algebraically closed field.

2.2.1. We first assume k to be an algebraic closure of $\mathbb{F}_p$ and proceed by induction. Observe that the canonical curve $\Sigma Z_\mu t^\mu$ can be written as $\Sigma Z_\mu t^\mu = E_0 + E_1 t + Z_2 t^2 + \ldots + Z_n t^n + \ldots$ So let H(n), $n \geq 1$ be the following inductionhypothesis:

H(n): Denoting $\underline{n} = [{}^p\log n]$ the unique integer such that $p^{\underline{n}} \leq n < p^{\underline{n}+1}$, there exist elements $X_0,\ldots,X_{\underline{n}}$ in Z and elements E_μ, $0 \leq \mu \leq n$ in $U(\underline{n}) = k\langle X_0,\ldots,X_{\underline{n}}\rangle \subset Z$ with the properties P1, P2, P3 below:

P1 : X_j is isobaric of weight p^j for $0 \leq j \leq \underline{n}$, $X_j = Z_{p^j} + u_j(Z_1,\ldots,Z_{p^{j-1}})$.

P2 : All E_μ are isobaric of weight μ. $E_0 = 1$, $E_{p^j} = X_j$, $0 \leq j \leq \underline{n}$.

P3 : The group H(Z) contains a curve γ_n, having the form:

$$\gamma_n = E_0 + E_1 t + \ldots + E_n t^n + x_{n+1} t^{n+1} + \ldots + x_j t^j + \ldots \tag{2.1}$$

such that all x_j are isobaric of weight j and such that the coefficient of Z_{p^m} in x_{p^m} is 1.

2.2.2. H(1) is true: $E_0 = 1$, $E_1 = X_0 = Z_1$. γ_1 is the canonical curve. Thus assume that H(n) holds for some $n \geq 1$ and take $E_1,\ldots,E_n$ as in P2. We distinguish the two cases: case A and case B.

Case A: n+1 is a power of p. Then $n+1 = p^{\underline{n+1}}$. Put $X_{\underline{n+1}} = x_{n+1}$ (2.1) and $E_{\underline{n+1}} = X_{\underline{n+1}}$. P3 gives that P1 is true in this case and P2 is trivial. Take $\gamma_{n+1} = \gamma_n$.

Case B: n+1 is not a power of p. Then $\underline{n+1} = \underline{n}$. We show the existence of $E_{n+1} \subset U(\underline{n})$, such that $dE_{n+1} = \sum_{\mu+\nu=n+1} E_\mu \otimes E_\nu$. Then $E_{n+1} - x_{n+1} \in P(Z)$ and we will be done using (1.6.8). In order to show the existence of E_{n+1} we first construct a curve $\Sigma C_\mu t^\mu$ satisfying certain conditions. Recall that if $\lambda \in k$ and $\gamma = \Sigma\gamma_\mu t^\mu$ is a curve in Z, then $\lambda * \gamma = \Sigma\lambda^\mu\gamma_\mu t^\mu \in H(Z)$. Thus let $\lambda \neq -1 \in k$ and consider the curve $\beta_n(\lambda) = \{\frac{1}{1+\lambda} * ((\lambda * \gamma_n).\gamma_n)\}.(-1) * \gamma_n$, i.e. denoting $\gamma_n = \Sigma A_\mu t^\mu$ (2.1) we have: $\lambda * \gamma_n = \Sigma\lambda^\mu A_\mu t^\mu$

$$(\lambda * \gamma_n).\gamma_n = (\Sigma\lambda^\mu A_\mu t^\mu)(\Sigma A_\mu t^\mu) = \sum_{i=0} \Big(\sum_{\mu+\nu=i} \lambda^\mu A_\mu A_\nu \Big) t^i$$

$$\frac{1}{1+\lambda} * ((\lambda * \gamma_n).\gamma_n) = \sum_{i=0} \Big(\sum_{\mu+\nu=i} \frac{\lambda^\mu A_\mu A_\nu}{(1+\lambda)^{\mu+\nu}} \Big) t^i$$

and finally:

$$\beta_n(\lambda) = \sum_{j=0} \Big(\sum_{\mu+\nu+\sigma=j} \frac{\lambda^\mu(-1)^\sigma}{(1+\lambda)^{\mu+\nu}} A_\mu A_\nu A_\sigma \Big) t^j = \sum_{j=0} B_j t^j.$$

This curve has the properties Q1,...,Q5:

Q1 : All B_j are isobaric of weight j. Indeed: all A_μ are isobaric of weight μ, by P3 if $\mu \geq n+1$ and by P2 if $\mu \leq n$. We adopt the convention that the zero element of Z has arbitrary weight.

Q2 : $B_{n+1} = \Big(\frac{\lambda^{n+1} + 1}{(1+\lambda)^{n+1}} + (-1)^{n+1}\Big) x_{n+1} + r(X_0,\ldots,X_{\underline{n}})$.

Obvious: take apart the solutions (μ,ν,σ) of $\mu+\nu+\sigma = n+1$ such that $(\mu,\nu,\sigma) \in \{(n+1,0,0),(0,n+1,0),(0,0,n+1)\}$. All other terms satisfy $0 \leq \mu,\nu,\sigma < n+1$ and are by P3 expressions in the $X_0,\ldots,X_{\underline{n}}$, and thus $r(X_0,\ldots,X_{\underline{n}}) \in U(\underline{n})$.

Q3 : There exists a $\lambda \in k$, such that $\zeta = \frac{\lambda^{n+1} + 1}{(1+\lambda)^{n+1}} + (-1)^{n+1} \neq 0$. This results from the fact that k is algebraically closed and n+1 is not a power of p.

Q4 : Considered as polynomials in the Z_i, we have:

$B_{p^j} = B_{p^j}(Z_1,\ldots,Z_{p^{j-1}})$ for every $j \geq 0$. Indeed: by the same argument of Q2 we see:

$$B_{p^j} = \left(\frac{\lambda^{p^j}+1}{(1+\lambda)^{p^j}} + (-1)^{p^j}\right)A_{p^j} + \text{isobaric expression in } A_1,\ldots,A_{p^j-1}$$

and the coefficient of A_{p^j} is zero for every prime p.

Q5 : $B_\mu \in U(\underline{n})$ if $0 \leq \mu \leq n$.

Now take $\lambda \in k$ such that $\zeta \neq 0$ (Q3). By the assumption on k we can find $\alpha \in k$ such that $\alpha^{n+1} = -\frac{1}{\zeta}$. Then $\alpha * \Sigma B_j t^j = \Sigma \alpha^j B_j t^j$. Taking the product of this curve with $\gamma_n = \Sigma A_i t^i$ we find a curve:

$$(2.2) \qquad \sum_{\mu=0} C_\mu t^\mu = \Sigma A_i t^i \cdot \Sigma \alpha^j B_j t^j = \sum_{\mu=0}\Big(\sum_{i+j=\mu} \alpha^j A_i B_j\Big)t^\mu.$$

with the properties R1,...,R4:

R1 : All C_μ are isobaric of weight μ. Obvious by Q1.

R2 : $C_{n+1} \in k<X_0,\ldots,X_{\underline{n}}> = U(\underline{n}) \subset Z$.

Indeed: $C_{n+1} = \alpha^{n+1}A_0B_{n+1} + \alpha^n A_1 B_n + \ldots + \alpha A_n B_1 + A_{n+1}B_0$

$$= \alpha^{n+1}(\zeta x_{n+1} + r(X_o,\ldots,X_{\underline{n}})) + \alpha^n E_1 B_n + \ldots + \alpha E_n B_1 + x_{n+1}$$

by Q2, Q3.

By choice of α we have $\alpha^{n+1}\zeta = -1$. By Q5 we are done.

R3 : Considered as elements of Z we have:

$C_{p^j} = Z_{p^j} + r_j$, $r_j \in k<Z_1,\ldots,Z_{p^{j-1}}>$, in particular $C_1 = Z_1$.

Indeed: $C_{p^j} = \alpha^{p^j}B_{p^j} + \alpha^{p^j-1}A_1 B_{p^j-1} + \ldots + \alpha A_{p^j-1}B_1 + A_{p^j}$.

B_{p^j} does not contain Z_{p^j} by Q4. By isobaricity the other terms cannot have Z_{p^j} except A_{p^j} and A_{p^j} contains the term Z_{p^j}, by P3 if $p^j \geq n+1$ and by P1 if $p^j < n+1$.

R4 : $C_\mu \in k<X_0,\ldots,X_{\underline{n}}> = U(\underline{n})$ for $0 \leq \mu \leq n+1$.

For $0 \leq \mu \leq n$ this follows from Q5 and the fact that $A_\nu = E_\nu$ if $0 \leq \nu \leq n$. For n+1 it is R2.

2.2.3. Construction of $E_{n+1} \in U(\underline{n})$ such that $E_{n+1} - x_{n+1} \in P(Z)$.

By the very definition of a curve, the curve $\Sigma C_\mu t^\mu$ defines a groupcoalgebraendomorphism, denoted ϕ, $\phi : Z \to Z$ such that $\phi(Z_\mu) = C_\mu$. Consider the induced groupendomorphism $H(\phi) : H(Z) \to H(Z)$ and in particular the curve

$$(2.3) \qquad H(\phi)(\gamma_n) = E_0 + \phi E_1 t + \ldots + \phi E_n t^n + \phi(x_{n+1})t^{n+1} + \ldots + \phi(x_j)t^j + \ldots$$

Now write $E_\mu = E_\mu(X_0,\ldots,X_{\underline{\mu}})$ as (noncommutative) polynomial function, and thus $\phi E_\mu = E_\mu(\phi X_0,\ldots,\phi X_{\underline{\mu}})$.

By P1 we have: $X_j = Z_{pj} + u_j(Z_1,\ldots,Z_{pj-1})$, $0 \leq j \leq \underline{n}$

thus $\phi X_j = C_{pj} + u_j(C_1,\ldots,C_{pj-1})$.

By R4 $\phi X_j = C_{pj}$ + polynomial in $X_0,\ldots,X_{j-1}$.

By R1 en R4 again: C_{pj} is a polynomial in $X_0,\ldots,X_j$ and so by R3 must contain a term X_j. We conclude

$$(2.4) \qquad \phi X_j = X_j + w_j(X_0,\ldots,X_{j-1}), \quad 0 \leq j \leq \underline{n}$$

and in particular: $\phi X_0 = \phi Z_1 = C_1 = Z_1 = X_0$.

The point is: By P3 we have: x_{n+1} is an isobaric expression in $Z_1,\ldots,Z_{n+1}$, denoted $x_{n+1} = f(Z_1,\ldots,Z_{n+1})$. Thus $\phi(x_{n+1}) = f(C_1,\ldots,C_{n+1})$ and by R4 we conclude: $\phi(x_{n+1}) = g(X_0,\ldots,X_{\underline{n}})$. But from (2.4) it follows: Every X_j can be expressed as a polynomial in $\phi X_0,\ldots,\phi X_j$ and if we assign to ϕX_i the weight p^i, X_i is an isobaric polynomial in the $\phi X_0,\ldots,\phi X_i$.

Substituting these in in the expression for $\phi(x_{n+1})$ we finally find:

(2.5) $\phi(x_{n+1}) = E_{n+1}(\phi X_0,\ldots,\phi X_{\underline{n}})$

where E_{n+1} is an isobaric polynomial in the ϕX_j.

The restriction $\rho_{\infty,n}\gamma_n = 1 + E_1 t +\ldots+ E_n t^n$ of γ_n defines a curve of order n in $Z(n) = k\langle Z_1,\ldots,Z_n\rangle \subset Z$, i.e. a groupcoalgebra endomorphism, denoted ψ, $\psi : Z(n) \to Z(n)$, $\psi(Z_i) = E_i$, $0 \leq i \leq n$. It thus follows that $\operatorname{Im}\psi = k[E_1,\ldots,E_n] = k\langle X_0,\ldots,X_{\underline{n}}\rangle = U(\underline{n})$ has a natural induced structure of groupcoalgebra over k, with diagonal d, $dX_i = \sum_{\mu+\nu=p^i} E_\mu \otimes E_\nu$, $0 \leq i \leq \underline{n}$.

From (2.4) it follows: $U(\underline{n}) = \operatorname{Im}\psi = k\langle X_0,\ldots,X_{\underline{n}}\rangle = k\langle\phi X_0,\ldots,\phi X_n\rangle$, that is to say, the restriction of ϕ to $\operatorname{Im}\psi$, denoted ϕ', is a groupcoalgebra automorphism of $U(\underline{n})$, i.e. we have a commutative diagram

$$\begin{array}{ccc} Z & \xrightarrow{\phi} & Z \\ \uparrow & & \uparrow \\ U(\underline{n}) & \xrightarrow[\sim]{\phi'} & U(\underline{n}) \end{array}$$

Now ϕ maps $x_{n+1} \in Z$ in fact in $U(\underline{n})$ in view of (2.5), and because ϕ' is an isomorphism we may consider the unique element

$$\phi'^{-1}\phi(x_{n+1}) = \phi'^{-1}E_{n+1}(\phi X_0,\ldots,\phi X_{\underline{n}}) \underset{\text{Def}}{=} E_{n+1}(X_0,\ldots,X_{\underline{n}}) \in U(\underline{n}).$$

Notice that $\phi : Z \to Z$ is in general not an automorphism of Z.

Now: a) $1 + E_1 t +\ldots+ E_n t^n + x_{n+1} t^{n+1}$ is a finite curve in Z (P3)

thus $1 + \phi E_1 t +\ldots+ \phi E_n t^n + \phi x_{n+1} t^{n+1}$ is a finite curve in $U(\underline{n})$

applying ϕ'^{-1}:

b) $1 + E_1 t +\ldots+ E_n t^n + E_{n+1} t^{n+1}$ is a finite curve in $U(\underline{n})$, hence is a finite curve in Z.

Comparing a) and b) we have:

$$d(E_{n+1} - x_{n+1}) = \sum_{\mu+\nu=n+1} E_\mu \otimes E_\nu - x_{n+1} \otimes 1 - 1 \otimes x_{n+1} - \sum_{\substack{\mu+\nu=n+1 \\ \mu,\nu\neq 0}} E_\mu \otimes E_\nu$$

$$= (E_{n+1} - x_{n+1}) \otimes 1 + 1 \otimes (E_{n+1} - x_{n+1})$$

thus $E_{n+1} - x_{n+1} \in P(Z)$.

2.2.4. Now apply lemma (1.6.8): $E_{n+1} - x_{n+1}$ is isobaric of weight n+1 ((2.5) and P3). There exists a curve $y = \Sigma y_m t^m$ in Z such that y_m is isobaric of weight m and $y \equiv 1 + (E_{n+1} - x_{n+1})t^{n+1} \pmod{t^{n+2}}$.

We now are in the position to verify H(n+1) in case B. Put

$$(2.6) \quad \gamma_{n+1} = \gamma_n . y = E_0 + E_1 t + \ldots + E_{n+1} t^{n+1} + u_{n+2} t^{n+2} + \ldots + u_j t^j + \ldots$$

This curve satisfies P3 of H(n+1): indeed, writing again $\gamma_n = \Sigma A_\mu t^\mu$ we have: $\gamma_{n+1} = \sum_{m=0} \left(\sum_{\mu+\nu=m} A_\mu y_\nu \right) t^m$. Because the A_μ and y_μ are isobaric of weight μ, γ_{n+1} has isobaric coefficients. Let m be such that $p^m \geq n+2$, then

$$u_{p^m} = A_{p^m} + A_{p^m-1} y_1 + \ldots + A_1 y_{p^m-1} + y_{p^m}.$$

By (1.6.8) $y_\mu = 0$ if μ is not a multiple of n+1, thus in case B: $y_{p^m} = 0$. The terms $A_\mu y_\nu$, $\mu \neq p^m$ cannot involve Z_{p^m}, but A_{p^m} does in view of P3 of H(n).

P2 of H(n+1) is obvious: We take $E_0, E_1, \ldots, E_{n+1}$ as the coefficients of t^μ, $0 \leq \mu \leq n+1$ in (2.6). P1 of H(n+1) is trivially true in case B. This finishes the proof of the existence theorem over an algebraically closed field.

2.2.5. Descent to the prime field $\mathbb{F}_p$.

Remark. (P. Cartier): Let $E = \Sigma E_\mu t^\mu$ be the curve of theorem 1 obtained over the algebraic closure of $\mathbb{F}_p$. Assume that for $0 \leq \mu \leq n$ we have: $E_\mu \in \mathbb{F}_p\langle X_0, \ldots, X_i, \ldots\rangle$ and $X_i \in \mathbb{F}_p\langle Z_1, Z_2, \ldots\rangle$ for $0 \leq i \leq n$. Considering

$$dE_{n+1} - E_{n+1} \otimes 1 - 1 \otimes E_{n+1} = \sum_{\substack{\mu+\nu=n+1 \\ \mu,\nu\neq 0}} E_\mu \otimes E_\nu$$

we see: the problem of descent is of linear nature and the right hand side is defined over $\mathbf{F}_p$. This guarantees that E_{n+1} can be chosen in $\mathbf{F}_p\langle X_0, X_1, \ldots, X_i, \ldots\rangle$. However, all author's attempts to prove the rationality of the E_μ along direct lines, using the natural base of monomials in the X_i failed on the noncommutativity of the problem. In order to obtain a rigorous proof we shall use the ordered p-bases of (1.6.3). All this will be carried out in 2§3. The author observes that P. Cartier found an alternative curve with the properties R1,...,R4 (2.2.2).

2§3 Descent to the prime field $\mathbf{F}_p$.

2.3.1. Definition. For a convenient terminology we shall say that the curve $\Sigma E_\mu t^\mu$ of th.1 (2.1.4) is the canonical E-pure curve over k. Any set of elements $(\xi_0, \xi_1, \ldots) \subset Z$ such that $\xi = \Sigma E_\mu(\xi_0, \ldots, \xi_\mu)t^\mu$ is a curve in Z will be called an E-pure set and ξ will be called the E-pure curve defined by the set $(\xi_0, \xi_1, \ldots)$. The element ξ_i in this set will be called an E-pure semiderivation of height i. By (1.5.3) we then have $V\xi_i = \xi_{i-1}$ for all $i \geq 0$, with the convention that $\xi_{-1} = 0$. By (1.5.6) we see that this agrees with the notion of semiderivation, introduced by J. Dieudonné in [7, page 242]. We recall the definition: Let B be a k-algebra, $\chi(k) = p > 0$. $\Delta : B \to B$ is a semiderivation of height r if Δ is k-linear, $\Delta(F^r B) \subset F^r B$ and if $\Delta(x^{p^r} y) = x^{p^r}\Delta(y) + y\,\Delta(x^{p^r})$. If $G \in \mathrm{GCoalg}_k$ we speak in the same way of E-pure sets, curves and semiderivations in G.

If $\phi = \Sigma\phi_\mu t^\mu$ is a curve in Z, then the induced groupendomorphism $H(\phi)$ of H(Z) (lemma 2.1.1) maps the canonical E-pure curve $\Sigma E_\mu(X_0, \ldots, X_\mu)t^\mu$ on the E-pure curve $\Sigma E_\mu(\phi X_0, \ldots, \phi X_\mu)t^\mu$. This curve will be called the E-pure curve belonging to ϕ and is as such defined by the E-pure set $(\phi X_0, \phi X_1, \ldots)$. It is clear that we can use the same terminology for finite E-pure curves $\Sigma^n E_\mu(\xi_0, \ldots, \xi_\mu)t^\mu$ defined by finite E-pure sets $(\xi_0, \ldots, \xi_n)$.

2.3.2. Notations. Z' will denote in this paragraph the $\mathrm{UNG}_{\mathbf{F}_p}$. k is an

algebraic closure of $\mathbb{F}_p$ and Z is the UNG_k. By P1 we have

$X_i = Z_{p^i} + u_i(Z_1,\ldots,Z_{p^{i-1}})$, $i \geq 0$ and $U = k\langle X_0,X_1,\ldots\rangle$;

$U(n) = k\langle X_0,\ldots,X_n\rangle \subset Z$. $U' = \mathbb{F}_p\langle X_0,X_1,\ldots\rangle$ and $U'(n) = \mathbb{F}_p\langle X_0,\ldots,X_n\rangle \subset Z$.

2.3.3. Sketch of the proof. Using induction we show the existence of an ordered p-base for Z, (q_{ij}), such that certain $q_{ij} \in Z'$ and such that all $\{q_{ij}\}_i$ are E-pure sets. It then is possible to write each u_i and E_μ uniquely as a sum a+b such that a is rational over $\mathbb{F}_p$ and $b \in P(Z)$. In view of (1.6.8) the term b can be cancelled out. That finishes the induction step and thus the u_i and the E_μ will be rational over $\mathbb{F}_p$.

2.3.4. Let $n \geq 1$ be an integer and let H'(n) be the following induction hypothesis:

H'(n) : The $u_j = u_j(Z_1,\ldots,Z_{p^{j-1}})$, $0 \leq j \leq n$ can be chosen such that $u_j \in Z'$ and the E_μ, $0 \leq \mu \leq n$ can be chosen such that $E_\mu \in U'(n) \subset Z'$.

Obviously H'(1) is true, because $E_0 = 1$ and $E_1 = X_0$, i.e. $u_0 = 0 \in Z'$. Thus assume H'(n) to be true for some $n \geq 1$ and let $u_j \in Z'$ if $0 \leq j \leq n$ and $E_\mu \in U'(n)$ if $0 \leq \mu \leq n$. As before we distinguish the cases A and B.

2.3.5. Case A: $n+1 = p^{n+1}$. We have already shown the existence of an ordered p-base for Z (1§6). As we shall see we may take the ordered p-base to consist of E-pure semiderivations. More precisely:

Lemma. Assuming H'(n), Z has an ordered p-base $Q = \{\eta_{ij} \mid i \geq 0,\ j \geq 1\}$ such that

a The sets $(\eta_{ij})_{i\geq 0}$ are E-pure for every $j \geq 1$.

b $\eta_{ij} \in Z'$ if $i \leq n$.

c The subset $\{\eta_{oj}\}_{j\geq 1}$ is a base for P(Z').

Proof. Take a base $\{\eta_{oj}\}_{j\geq 1}$ for P(Z'). By lemma (1.6.7) there exist curves

$x_j = \Sigma x_{\mu j} t^{\mu} \in Z'$ such that $x_{1j} = \eta_{oj}$ for all $j \geq 1$. Consider the x_j as curves in Z and let η_j be the E-pure curve belonging to x_j, defined by the E-pure set $(\eta_{ij})_{i \geq 0}$. We claim: the set $Q = \{\eta_{ij} \mid i \geq 0, j \geq 1\}$ is an ordered p-base for Z. Indeed: in view of (1.5.6), applied to the curves η_j, we may conclude by (1.6.6 corollary 2).(Observe that $P(Z') \subset Z$ and $P(Z) = k \otimes_{F_p} P(Z')$, thus $\{\eta_{oj}\}_{j \geq 1}$ is indeed a base for P(Z).)
For b we have by H'(n):

$$(2.7) \qquad \eta_{ij} = x_{p^i,j} + u_i(x_{1,j},\ldots,x_{p^{i-1},j}) \in Z' \text{ for } 0 \leq i \leq n,\ j \geq 1.$$

and the lemma is proven.

Notation. The resulting base for the k-vectorspace Z,defined by Q will be denoted by $Y = \{\eta_\alpha \mid \alpha \in T\}$. T is an index set which can be described as follows: Let $I = \{(i,j) \mid i,j \in Z,\ i \geq 0,\ j \geq 1\}$ then $T = \{(\alpha_{i,j}) \mid (i,j) \in I,\ 0 \leq \alpha_{ij} < p$, almost every α_{ij} is zero$\}$. We put $Y' = \{\eta_\alpha \in Y \mid \eta_\alpha$ is product of $\eta_{ij} \in Q,\ 0 \leq i \leq n\}$. Thus in particular: $Y' \subset Z'$. Let $T' = \{\alpha \in T \mid \eta_\alpha \in Y'\}$. We now have in our case A:

$$(2.8) \qquad u_{n+1}(Z_1,\ldots,Z_n) = \sum_{\alpha \in T} \lambda_\alpha \eta_\alpha,\ \lambda_\alpha \in k.$$

A first slight refinement of (2.8) is:

2.3.6. Lemma. $u_{n+1} = \sum_{\alpha \in T'} \lambda_\alpha \eta_\alpha,\ \lambda_\alpha \in k.$

Proof. First remark that if M is a monomial in the Z_μ, then $VM \neq 0$ implies $\omega(VM) = \frac{1}{p}\omega(M)$. It now follows by $V^i \eta_{ij} = \eta_{oj} \neq 0$ that η_{ij}, considered as an expression in the Z_μ has weight at least p^i. Because the u_i are isobaric of weight p^i, we now have:

$$u_{n+1} = \sum_s \mu_s \eta_{n+1,s} + \sum_{\alpha \in T'} \lambda_\alpha \eta_\alpha;\ \lambda_\alpha, \mu_s \in k.$$

Apply V^{n+1}. Then $V^{n+1} u_{n+1} = V^{n+1}(X_{n+1} - Z_{n+1}) = X_0 - Z_1 = X_0 - X_0 = 0$ and

$\overline{V^{n+1}}(\eta_\alpha) = 0$ if $\alpha \in T'$. By the linear independency of the $\overline{V^{n+1}}(\eta_{\underline{n+1},s}) = \eta_{o,s}$ we are done.

2.3.7. Corollary. If $x \in Z$ is isobaric of weight $\leq n$, then $x = \sum_{\alpha \in T'} \mu_\alpha \eta_\alpha$, $\mu_\alpha \in k$. If moreover $x \in Z'$, then $\mu_\alpha \in \mathbb{F}_p$.

Proof. The first statement results immediately from the observation: η_{ij} has at least weight p^i. Now let $\{\xi_\alpha \mid \alpha \in T\}$ be the base of monomials in the Z_μ for Z, then if $\alpha \in T'$, $\eta_\alpha \in Z'$ and thus $\eta_\alpha = \Sigma_\beta \sigma_{\alpha\beta}\xi_\beta$, $\sigma_{\alpha\beta} \in \mathbb{F}_p$.
Moreover: $x \in Z'$ implies $x = \Sigma_\beta \rho_\beta \xi_\beta$, $\rho_\beta \in \mathbb{F}_p$.
Thus $\Sigma_\beta \rho_\beta \xi_\beta = x = \sum_{\alpha \in T'} \mu_\alpha \eta_\alpha = \sum_{\alpha,\beta} \mu_\alpha \sigma_{\alpha\beta} \xi_\beta$. By the linear independency of the ξ_β and the η_α, the matrix $\sigma = (\sigma_{\alpha\beta})$ is invertible.
Writing (μ_α) as a columnvector μ and (ρ_β) as a columnvector ρ, we have:
$\mu = \rho\sigma^{-1}$ is rational over $\mathbb{F}_p$, hence $\mu_\alpha \in \mathbb{F}_p$.

2.3.8. Define $\Delta : Z \to Z \otimes_k Z$ by $\Delta x = dx - x \otimes 1 - 1 \otimes x$. Then Δ is obviously k-linear. We use (2.3.7) to arrive at the important corollary:

Corollary. $\Delta u_{\underline{n+1}} = \sum_{\alpha,\beta \in T'} \lambda_{\alpha\beta} \eta_\alpha \otimes \eta_\beta$, $\lambda_{\alpha\beta} \in \mathbb{F}_p$.

Proof. $\Delta u_{\underline{n+1}} = \sum_{\substack{\mu+\nu=n+1 \\ \mu,\nu \neq 0}} (E_\mu \otimes E_\nu - Z_\mu \otimes Z_\nu)$. All E_μ, Z_ν involved are isobaric of weight $\leq n$ and belong to Z' (by $H'(n)$). Thus apply (2.3.7).

2.3.9. Lemma. Write $u_{\underline{n+1}} = \sum_{\alpha \in A \subset T'} \lambda_\alpha \eta_\alpha + \sum_{\beta \in B \subset T'} \mu_\beta \eta_\beta$, $\lambda_\alpha \in \mathbb{F}_p$, $\mu_\beta \notin \mathbb{F}_p$, $A \cap B = \emptyset$. Then $w = \sum_{\beta \in B} \mu_\beta \eta_\beta \in P(Z)$.

Proof. Observe that by (2.3.6) such an expression for $u_{\underline{n+1}}$ is justified. Now η_β is an ordered product of η_{ij}, thus each η_β can uniquely be written as $\eta_\beta = r_\beta s_\beta$, such that r_β is product of semiderivations of constant height i_0 and s_β is product of semiderivations η_{ij} such that $i < i_0$. Select from $w = \Sigma_\beta \mu_\beta r_\beta s_\beta$ the unique subsum of all terms such that i_0 is maximal.

Choose $r = r_\beta$ and collect from this subsum all terms $\mu_\gamma r_\gamma s_\gamma$ such that $r_\gamma = r$. Moreover assume r to be chosen such that the number of factors $\eta_{i_0 j}$ in r is maximal. We then find a subsum of w, say $t = r(\mu_1 s_1 + \ldots + \mu_m s_m)$. Observe that by E-purity of the η_{ij} we have for $0 \leq i \leq n$:

$$d\eta_{ij} = \eta_{ij} \otimes 1 + 1 \otimes \eta_{ij} + f(\eta_{ij})$$

where $f(\eta_{ij})$ is rational over $\mathbb{F}_p$ and contains only $\eta_{\mu j}$ such that $\mu < i$.

It follows, because dt is again a subsum of dw: dw contains the term $\mu_1 r \otimes s_1 + \ldots + \mu_m r \otimes s_m$. On the other hand $\Delta w = \Delta u_{\underline{n+1}} - \Delta \sum_{\alpha \in A} \lambda_\alpha \eta_\alpha$ is rational over $\mathbb{F}_p$. Thus the term $r \otimes (\mu_1 s_1 + \ldots + \mu_m s_m)$ must have been cancelled out in Δw. In view of the maximal choice of r and the fact that the set $\{\eta_\alpha \otimes \eta_\beta \mid \alpha,\beta \in T'\}$ is linear independent over k, it now follows that, writing $\Delta w = dw - w \otimes 1 - 1 \otimes w$, we must have $r \otimes (\mu_1 s_1 + \ldots + \mu_m s_m)$ contributes to $w \otimes 1$, i.e. $m = 1$ and thus t reduces to a single term, say $t = \mu r$, where r is a product of semiderivations of constant height i_0. If $i_0 \geq 1$ we see that $Vu_{\underline{n+1}} = X_{\underline{n}} - Z_{p\underline{n}}$ contains a term $V(\mu r) = \mu^{p-1}.Vr$ where $\mu^{p-1} \notin \mathbb{F}_p$. By linear independence and the hypothesis H'(n) this is not possible unless $Vr = 0$, i.e. $i_0 = 0$ and r is a product of $\eta_{oj} \in P(Z')$. By the maximality of the choice of i_0 we arrive at:

$$w = \sum_\beta \mu_\beta \eta_\beta, \quad \eta_\beta = \prod_j \eta_{oj}^{\beta_j}, \quad 0 \leq \beta_j < p, \quad \mu_\beta \notin \mathbb{F}_p.$$

Put $\eta'_\beta = \frac{\eta_\beta}{\prod \beta_j!}$, then $w = \sum_\beta \mu'_\beta \eta'_\beta$, $\mu'_\beta \notin \mathbb{F}_p$ and by the known Leibniz-rules we have $dw = \sum_\beta \sum_{\alpha+\gamma=\beta} \mu'_\beta \eta'_\alpha \otimes \eta'_\gamma$.

By the linear independence of the $\eta'_\alpha \otimes \eta'_\gamma$ we now conclude: w is rational over $\mathbb{F}_p$ iff $w \in P(Z)$.

2.3.10. Proposition. H'(n+1) is true if $n+1 = p^{\underline{n+1}}$.

Proof. We follow the proof of case A in theorem 1. Consider γ_n (2.1)

$\gamma_n = E_0 + E_1 t + \ldots + E_n t^n + x_{n+1} t^{n+1} + \ldots$ where $x_{n+1} = Z_{n+1} + u_{\underline{n+1}}$. By (2.3.9) we have $u_{\underline{n+1}} = v + w$ such that $v \in Z'$, $w \in P(Z)$. By (1.6.7) there exists a curve γ' in Z such that $\gamma' \equiv 1 - wt \pmod{t^2}$. Consider in the proof of case A, theorem 1, the curve

$$\gamma_n \cdot V_{n+1}\gamma' = E_0 + E_1 t + \ldots + E_n t^n + (x_{n+1} - w)t^{n+1} + \ldots$$

and put $X'_{\underline{n+1}} = x_{n+1} - w = Z_{n+1} + v \in Z'$. Write $X'_{\underline{n+1}} = X_{\underline{n+1}} + \partial$ where $X_{\underline{n+1}}$ is the homogeneous part of weight n+1, and ∂ contains no terms of weight n+1. It is easily seen that $\partial \in P(Z')$. Using the arguments of (1.6.8) we can construct a curve

$\gamma_{n+1} = E_0 + E_1 t + \ldots + E_n t^n + X_{\underline{n+1}} t^{n+1} + x'_{n+2} t^{n+2} + \ldots + x'_j t^j + \ldots$ such that x'_j is isobaric of weight j. Because $V^m x'_{p^m} = X_0 = Z_1$ it follows by isobaricity that x'_{p^m} contains Z_{p^m} with coefficient 1. We thus have shown that H(n) and H'(n) imply H(n+1) and H'(n+1) if $n+1 = p^{\underline{n+1}}$.

2.3.11. Case B, $p^{\underline{n}} < n+1 < p^{\underline{n+1}}$.

The line of the proof is analoguous to the proof of case A. Observe first that assuming H'(n), $U'(\underline{n}) = \mathbb{F}_p\langle X_0, \ldots, X_{\underline{n}}\rangle$ has a natural induced structure of $\mathbb{F}_p$-groupcoalgebra, with diagonal d, $dX_i = \sum_{\mu+\nu=p^i} E_\mu \otimes E_\nu$, $0 \leq i \leq \underline{n}$. Because the induced natural filtration on $U'(\underline{n})$ as a subgroupcoalgebra of Z' is exhaustive, $U'(\underline{n})$ is infinitesimal (lemma 1.3.5).

Moreover $U'(\underline{n})$ has finite height: Let $x \in \mathrm{Ker}\{\varepsilon : U'(\underline{n})^* \to \mathbb{F}_p\}$, then for every $u \in U'(\underline{n})$ we have $\langle x^{p^{\underline{n+1}}}, u\rangle = \langle x, V^{\underline{n+1}} u\rangle^{p^{\underline{n+1}}} = 0$ because $\mathrm{Im}\, V^{\underline{n+1}} = \eta(\mathbb{F}_p) \subset U'(\underline{n})$. By (1.3.9) we conclude: $U'(\underline{n})^*$ is isomorphic with a truncated powerseries algebra over $\mathbb{F}_p$.

By (1.6.6), corollary 1 we conclude the existence of an ordered p-base $Q = \{\eta_{ij} \mid j \geq 1,\ 0 \leq i \leq N(j) \leq \underline{n}\}$ for $U'(\underline{n})$ over $\mathbb{F}_p$, and we clearly may assume that the η_{ij} are E-pure semiderivations. (Take in the proof of (1.6.6), corollary 1 instead of the ψ_j the finite E-pure curves belonging

to ψ_j).

We now have: $E_\mu \in U'(\underline{n})$ if $0 \leq \mu \leq n$ and $E_{n+1} \in U(\underline{n}) = k \otimes_{\mathbb{F}_p} U'(\underline{n})$. Because the ordered p-base Q defines a base $Y = \{\eta_\alpha \mid \alpha \in T\}$ for $U'(\underline{n})$ over $\mathbb{F}_p$ as well for $U(\underline{n})$ over k, we again can write uniquely

$$E_{n+1} = \sum_{\alpha \in A \subset T} \lambda_\alpha \eta_\alpha + \sum_{\beta \in B \subset T} \mu_\beta \eta_\beta,\ \lambda_\alpha \in \mathbb{F}_p,\ \mu_\beta \notin \mathbb{F}_p,\ A \cap B = \emptyset$$

and ΔE_{n+1} is rational over $\mathbb{F}_p$. We now can repeat litterally the proof of (2.3.9) in order to show: $w = \sum_\beta \mu_\beta \eta_\beta \in P(U(\underline{n}))$.

Now consider in Z again the curve γ_{n+1}, (2.6)

$$\gamma_{n+1} = E_0 + E_1 t + \ldots + E_{n+1} t^{n+1} + u_{n+2} t^{n+2} + \ldots + u_j t^j + \ldots$$

Taking a curve γ' in Z such that $\gamma' \equiv \gamma - wt \pmod{t^2}$, consider the curve

$$\gamma_{n+1} \cdot V_{n+1} \gamma' = E_0 + E_1 t + \ldots + E_n t^n + (E_{n+1} - w) t^{n+1} + \ldots$$

By the same reasoning as in (2.3.10) we now can find a curve

$$(2.9) \qquad \gamma'_{n+1} = E_0 + E_1 t + \ldots E_n t^n + E'_{n+1} t^{n+1} + u'_{n+2} t^{n+2} + \ldots + u'_j t^j + \ldots$$

such that E'_{n+1} is isobaric of weight n+1 and the u'_j are isobaric of weight j. We take as new E_{n+1} the coefficient E'_{n+1} of t^{n+1} in the curve γ'_{n+1}. This coefficient is rational over $\mathbb{F}_p$, and, by construction, belongs to $U'(\underline{n})$: indeed $E_{n+1} - w \in U'(\underline{n})$ and because d on $U'(\underline{n})$ is compatible with the weightfunction we can write uniquely $E_{n+1} - w = E'_{n+1} + \partial$ where E'_{n+1} is isobaric of weight n+1 and $\partial \in P(U'(\underline{n})) \subset P(Z')$ does not contain any term of weight n+1. We now have in case B: H(n) and H'(n) imply H(n+1) and H'(n+1), thus the existence theorem is completely proven.

Remark. It should be noted that J.A. Dieudonné had already obtained the groupcoalgebra $U = \mathbb{F}_p\langle X_0, X_1, \ldots\rangle$, however by different methods. [5], see especially the review of P. Cartier [MR 20-930]: With the notation of

the review: $\mathcal{F}_1(k) = U$ and $\mathcal{H}_1(k) = Z$. The difference between the two approaches can be made more clear by the following observation:

Let G be a hyperalgebra over k in the sense of Dieudonné [MR 20-930], then by definition the linear dual G^* is isomorphic with a formal powerseries algebra $k[[Y_i]]_{i \in T}$ for a suitable index set T. Now consider in our notations $Al_k(G^*, k[[t_i]]_{i \in T})$. Let the set of all monomials in the t_i be $\{t^\alpha\}_{\alpha \in S}$ for a suitable index set S, then this set has a natural structure of abelian monoid and $\phi : G^* \to k[[t_i]]_{i \in T}$ is completely determined by $\phi(x) = \sum_{\alpha \in S} \phi_\alpha(x) t^\alpha$, $\phi_\alpha \in G$, $x \in G^*$.

It is clear that the $\{\phi_\alpha\}_{\alpha \in S}$ is a base for the k-vectorspace G and is a structural base for G, i.e. $d(\phi_\alpha) = \sum_{\beta+\gamma=\alpha} \phi_\beta \otimes \phi_\gamma$.

In the approach of Dieudonné, hyperalgebras are handled as k-vectorspaces, carrying certain additional structures, and it seems never to have been mentioned that the set of structural bases of G, i.e., more exactly, the set $Al_k(G^*, k[[t_i]]_{i \in T})$, carries a natural groupstructure. It turns out however that the group $Al_k(G^*, k[[t]])$ contains already all essential information that is needed. By the existence theorem one knows the most simple elements of this group, namely E-pure curves. In Chapter III we shall use these E-pure curves in order to obtain a decomposition of arbitrary curves in a product of E-pure curves and to recover the Campbell-Hausdorff-Dieudonné theorem.

CHAPTER III

Properties of U and Z

We write GCoalg instead of $GCoalg_{\mathbb{F}_p}$.

3.1.1. The existence theorem gives immediately:

Proposition. Define on $U = \mathbb{F}_p\langle X_0, X_1, \ldots\rangle$ the weightfunction $\omega : U \to \mathbb{Z}$ by $\omega(X_i) = p^i$, $\omega(xy) = \omega(x) + \omega(y)$ if $x,y \in U$. Let $E = \Sigma E_\mu t^\mu$ be the E-pure curve of the existence theorem (2.1.4). Then E defines on U a structure of $\mathbb{F}_p$-groupcoalgebra and for all $i \geq 0$:

$$dX_i = \sum_{\mu+\nu=p^i} E_\mu \otimes E_\nu$$

$$\varepsilon X_i = 0.$$

Remark on the proof. Let Z be the UNG in GCoalg, then U is isomorphic with Im $(E : Z \to Z)$, $E(Z_i) = E_i$. The diagonal d and augmentation ε are obtained from restriction of $d : Z \to Z \otimes Z$ and $\varepsilon : Z \to \mathbb{F}_p$ to Im E.

Notice that the formulae (p1 of (2.2.1)), written as

$$j(X_i) = Z_{p^i} + u_i(Z_1, \ldots, Z_{p^{i-1}})$$

define an embedding $j : U \hookrightarrow Z$ in GCoalg. The E_μ are not unique, but the groupcoalgebra structure on U is independent of the choice of the E_μ in view of the lemma:

3.1.2. Lemma. Let $F = \Sigma F_\mu t^\mu$ be a curve in $Z \in GCoalg$ such that F_μ is isobaric of weight μ, $\mu \geq 0$, $F_1 \neq 0$ and Im F is generated over $\mathbb{F}_p$ by the F_{p^i}, $i \geq 0$. Then the composed morphism $U \overset{j}{\hookrightarrow} Z \overset{F}{\to}$ Im F is an isomorphism in GCoalg and Im $F = \mathbb{F}_p\langle F_1, F_p, \ldots, F_{p^i}, \ldots\rangle$.

Proof. $F \circ j(X_i) = F(Z_{p^i} + u_i(Z_1, \ldots, Z_{p^{i-1}})) = F_{p^i} + u_i(F_1, \ldots, F_{p^{i-1}})$. By

isobaricity, the $F_\mu \in \mathrm{Im}\, F$ can only be expressions in the F_{p^j} such that $p^j \leq \mu$, thus $F \circ j(X_i) = F_{p^i} + w_i(F_1, F_p, \ldots, F_{p^{i-1}})$. It follows that the F_{p^i} can be expressed in the $F \circ j(X_i)$, i.e. $F \circ j$ is surjective. $F_1 = \alpha Z_1$ $\alpha \neq 0$, $\alpha \in \mathbb{F}_p$ (by isobaricity), $\Sigma F_\mu t^\mu$ is a curve, and thus by (1.5.3), $VF_{p^i} = F_{p^{i-1}}$ and $V^i F_{p^i} = F_1 = \alpha Z_1$.
In view of the relations $VZ_\mu = 0$ if $(\mu,p) = 1$, $VZ_{\mu p} = Z_\mu$ it follows that F_{p^i} contains a term $\alpha^{p^i} Z_{p^i}$. From isobaricity we now deduce that the F_{p^i} are independent generators for $\mathrm{Im}\, F$ over $\mathbb{F}_p$, i.e. $\mathrm{Im}\, F = \mathbb{F}_p\langle F_1, F_p, \ldots, F_{p^i}, \ldots\rangle$. Because U itself is a free algebra too, $F \circ j$ is injective. It then is clear that $F \circ j$ is an isomorphism in GCoalg.

3.1.3. Definition. The object in GCoalg, defined up to isomorphism by any curve $\Sigma F_\mu t^\mu$ in Z, satisfying to the conditions of lemma (3.1.2) will be called the noncommutative exponential groupcoalgebra over $\mathbb{F}_p$, abbreviated NEG over $\mathbb{F}_p$. In the sequel we fix once for all the canonical E-pure curve $E = \Sigma E_\mu t^\mu$ and represent the NEG over $\mathbb{F}_p$ by $U = \mathbb{F}_p\langle X_0, X_1, \ldots\rangle$ as done in (3.1.1). Notice that the analoguous object U over the field of rational numbers is given by $U = \mathbb{Q}[X]$, $dX = X \otimes 1 + 1 \otimes X$, i.e. the bialgebra of the additive group.

3.1.4. A first justification of the term exponential is given by:

Lemma. There exists a $\mathbb{F}_p$-derivation $\partial : U \to U$ such that $\partial E_\mu = E_{\mu-1}$, $\mu \geq 1$. As a consequence, extending ∂ to a $\mathbb{F}_p[[t]]$-derivation of $U[[t]]$, we have for the canonical E-pure curve E : $\partial E = Et$.

Proof. Take the base $\{M_\alpha\}_{\alpha \in S}$ of monomials in the X_i in U and let $\{N_\beta\}_{\beta \in S} \subset U^*$ be the set of pointdistributions on the M_α. Let in particular $\langle N_\alpha, X_0\rangle = 1$. Then in $U^\vee$ we have by Cartierduality $dN_\alpha = N_\alpha \otimes 1 + 1 \otimes N_\alpha$. Let ∂ be the composite map

$$U \to U \otimes U \xrightarrow{1 \otimes N_\alpha} U \otimes \mathbb{F}_p \xrightarrow{\sim} U$$

then ∂ is a $\mathbb{F}_p$-derivation and $\partial(E_\mu) = (1 \otimes N_\alpha)(\sum_{\rho+\sigma=\mu} E_\rho \otimes E_\sigma) = E_{\mu-1}$ if $\mu \geq 1$.

In particular $\partial X_i = \partial E_{p^i} = E_{p^{i-1}}$.

Notice that the analoguous assertion over $\mathbb{Q}$ is trivial.

3.1.5. Lemma. Let $\mathcal{A}$ be the two sided ideal in U generated by all commutators $[X_i, X_j]$. Denote by Y_i resp. G_μ the classes of X_i resp. E_μ modulo $\mathcal{A}$. Then $A = U/\mathcal{A}$ has a natural induced structure of abelian groupcoalgebra over $\mathbb{F}_p$ and the G_μ are uniquely determined by the relation

$$(3.1) \quad \sum_{\mu=0}^{\infty} G_\mu t^\mu = \sum_{\mu=0}^{\infty} G_\mu(Y_0,\ldots,Y_\mu)t^\mu = \mathrm{Hex}(Y_0 t,\ldots,Y_i t^{p^i},\ldots) \quad [3,\text{pag } 60].$$

In particular the hyperexponential series of J. Dieudonné defines on A a structure of abelian $\mathbb{F}_p$-groupcoalgebra which is identical with the quotientstructure on $A = U/\mathcal{A}$.

Proof. It is a trivial verification that $d\mathcal{A} \subset U \otimes \mathcal{A} + \mathcal{A} \otimes U$, and $\varepsilon(Y_1) = 0$. Let $\mathrm{Hex}(Y_0 t,\ldots,Y_i t^{p^i},\ldots) = \sum_{\mu=0}^{\infty} F_\mu t^\mu$, then the F_μ define on A a structure of abelian groupcoalgebra. $d' : A \to A \otimes A$ is given by

$$d'Y_i = \sum_{\mu+\nu=p^i} F_\mu \otimes F_\nu. \quad (1.2.6f).$$

Both the F_μ and the G_μ are isobaric of weight μ with respect to the induced weightfunction, again denoted ω, $\omega(Y_i) = p^i$; $F_0 = G_0 = 1$ and $F_{p^i} = G_{p^i} = Y_i$ for $i \geq 0$. For the F_μ this results from J. Dieudonné [3, pag 60].

Let the quotientstructure on A be given by $d : A \to A \otimes A$, then $dY_0 = d'Y_0 = Y_0 \otimes 1 + 1 \otimes Y_0$. Thus let $n \geq 0$ and assume that the restrictions of the (A,d)- and (A,d')-structure to the subgroupcoalgebra $A(n) = \mathbb{F}_p[Y_0,\ldots,Y_n]$ are identical, i.e.: $G_\mu = F_\mu$ for all $0 \leq \mu \leq p^n$. Suppose there exists m, $p^n < m \leq p^{n+1}$ such that $G_m \neq F_m$.

Take m as small as possible and assume first that $p^n < m < p^{n+1}$. Then $G_m \in A(n)$, $d(G_m) = d'(G_m)$ and $d(F_m) = d'(F_m)$. Moreover $d(G_m - F_m) = d'(G_m - F_m) = (G_m - F_m) \otimes 1 + 1 \otimes (G_m - F_m)$, i.e. $G_m - F_m \in P(A(n))$ and $G_m - F_m$ is isobaric of weight m. Admitting for the moment the fact $P(A(n)) = \bigoplus_{i=0}^{\infty} \mathbb{F}_p Y_0^{p^i}$, we conclude: $p^n < m < p^{n+1}$ is not possible, thus we should have $m = p^{n+1}$. But then $G_m = F_m = Y_{n+1}$, thus $G_\mu = F_\mu$ for all $\mu \geq 0$.

Now let $u = a_0 + a_1 Y_i + \ldots + a_m Y_i^m \in P(A(n))$, $0 \leq i \leq n$, $a_j \in A(i-1)$, $a_m \neq 0$. du contains a term $a_m \otimes Y_i^m$ and $du = u \otimes 1 + 1 \otimes u$. It thus follows that $a_m \in \mathbb{F}_p$. Because $\Sigma G_\mu t^\mu$ is a curve in A, we have $VY_i = VG_{p^i} = G_{pi-1} = Y_{i-1}$ if $i \geq 0$ and $VY_0 = 0$ (1.5.3). Thus applying V to u we have $0 = Va_0 + Va_1 . Y_{i-1} + \ldots + Va_m . Y_{i-1}^m$. Notice that $1 + ut$ is a curve, thus by (1.5.3), $Vu = 0$. Because $0 \neq a_m \in \mathbb{F}_p$, we have $Va_m = a_m^{1/p} = a_m \neq 0$. Hence $i = 0$ and $u = a_0 + \ldots + a_m Y_0^m$, $a_i \in \mathbb{F}_p$.
Using $dY_0 = Y_0 \otimes 1 + 1 \otimes Y_0$, one now easily checks that $u \in \bigoplus_{i=0}^{\infty} \mathbb{F}_p Y_0^{p^i}$.

3.1.6. Corollary. There exists a $\mathbb{F}_p$-derivation $\partial : A \to A$ such that $\partial G_\mu = G_{\mu-1}$ for $\mu \geq 1$. In particular $\partial \mathrm{Hex}(Y_0, \ldots, Y_i, \ldots) = \mathrm{Hex}(Y_0, \ldots Y_i, \ldots)$.

Proof. Because the derivation ∂ of (3.1.4) satisfies $\partial(\mathfrak{a}) \subset \mathfrak{a}$, ∂ induces a derivation on the quotient $A = U/\mathfrak{a}$.

The hyperexponential series $\mathrm{Hex}(Y_0 t, \ldots, Y_i t^{p^i}, \ldots)$ will be denoted in future again by $\Sigma E_\mu t^\mu = \Sigma E_\mu(Y_0, \ldots, Y_\mu) t^\mu$. This is consistent with the previous notations, because every E-pure curve in $G \in \mathrm{Ab}_{\mathbb{F}_p}$, i.e. every morphism $U \to G$ factorizes uniquely through A. We write $E_\mu(Y_0, \ldots, Y_\mu)$ instead of $E_\mu(Y_0, \ldots, Y_\mu)$. One now has the important fact, already observed by J. Dieudonné [3, pag. 60]:

3.1.7. Lemma. Let $\xi = \Sigma E_\mu(\xi_0, \ldots, \xi_\mu) t^\mu$ and $\eta = \Sigma E_\mu(\eta_0, \ldots, \eta_\mu) t^\mu$ be two curves in an abelian groupcoalgebra $G \in \mathrm{Ab}_k$, then $\xi\eta$ and ξ^{-1}, considered as elements of the group H(G), are again E-pure.

Remark on the proof. This is a restatement of

$\mathrm{Hex}(Y_0,\ldots,Y_i,\ldots)\ \mathrm{Hex}(T_0,\ldots,T_i,\ldots) = \mathrm{Hex}(S_0,\ldots,S_i,\ldots)$ where

$S_i = \Sigma E_\mu(Y_0,\ldots,Y_\mu)\ E_\nu(T_0,\ldots,T_\nu)$. [3, pag. 60]. Here Σ means $\sum_{\mu+\nu=p^i}$.

Let C be a category and let GC be the category of all commutative group-objects in C. If $X \in GC$ then X is a cogroupobject in GC.

Now if $G \in \mathrm{Ab}_k$, there exists a canonical bijection $\mathrm{Ab}_k(A,G) \overset{\sim}{\to} \mathrm{GCoalg}_k(U,G) \overset{\sim}{\to}$ {Set of E-pure curves in G}, functorial in G.

In view of the foregoing, A is a cogroupobject in Ab_k and thus $\mathrm{Ab}_k(A,G)$ is a commutative group, functorial in $G \in \mathrm{Ab}_k$.

If $\xi,\eta \in \mathrm{Ab}_k(A,G)$, and if ξ and η are considered as two E-pure curves, then their "sum" $\phi\psi$ in the group $\mathrm{Ab}_k(A,G)$ is given by

$A \to A \otimes A \xrightarrow{\phi \otimes \psi} G \otimes G \to G$ and thus must be an E-pure curve again. In view of this, the lemma is evident.

3.1.8. For reference we mention the theorem of Dieudonné [6, formula 25].

Theorem. The bialgebra of the Witt vectors of infinite length over $\mathbb{F}_p$ and the abelian groupcoalgebra A are isomorphic in GCoalg.

Likewise the bialgebra $A(W_n)$ of Witt vectors of length n and the subgroup-coalgebra $A(n-1) = k[Y_0,\ldots,Y_{n-1}] \subset A$ are isomorphic in GCoalg.

3§2 The decomposition theorem over a field k, $\chi(k) = 0$.

For convenience in comparing the cases $\chi(k) = p > 0$ and $\chi(k) = 0$ we first consider the essentially known case $\chi(k) = 0$. We use the exponential series, defined by $\exp u = \sum_{i=0}^{\infty} \frac{u^i}{i!}$ if u belongs to a suitable Q-algebra.

3.2.1. Theorem. (decomposition theorem in characteristic 0). Let k be a field, $\chi(k) = 0$ and let Z be the UNG over k. Then there exists a unique family $(Y_i)_{i\geq 1} \subset P(Z)$, such that:

a $Y_i = Z_i + v_i(Z_1,\ldots,Z_{i-1})$ is isobaric of weight i, $i \geq 1$.

b $\Sigma Z_\mu t^\mu = \prod_{i=1}^{\infty} \exp(Y_i t^i)$ in $H(Z)$.

Note: because the situation is not commutative, every product will denote an ordered product. The order in (3.2.1)b is the natural order of the integers.

Proof. First remark that the infinite product is defined in H(Z), cf. (1.4.11). As starting point for an induction argument observe that

$$\Sigma Z_\mu t^\mu \equiv \exp(Z_1 t) \pmod{t^2}.$$

Put $Y_1 = Z_1$. Now assume that for some integer $n \geq 1$ the following holds: There exist $Y_i = Z_i + v_i(Z_1,\ldots,Z_{i-1})$, $1 \leq i \leq n$, such that all Y_i are isobaric and $Y_i \in P(Z)$ and such that

$$\Sigma Z_\mu t^\mu \equiv \prod_{i=1}^{n} \exp(Y_i t^i) \pmod{t^{n+1}}.$$

(Observe that $\exp(Y_i t^i) = V_i \exp(Y_i t)$ (1.4.9) is indeed a curve in Z). Let D_{n+1} be the coefficient of t^{n+1} in $\prod_{i=1}^{n} \exp(Y_i t^i)$, then D_{n+1} is isobaric of weight n+1 and $Z_{n+1} - D_{n+1} \in P(Z)$ because both curves agree up to the coefficient of t^n. Putting $Y_{n+1} = Z_{n+1} - D_{n+1}$ one has obviously $Y_{n+1} = Z_{n+1} + v_{n+1}(Z_1,\ldots,Z_n)$ and

$$\Sigma Z_\mu t^\mu \equiv \prod_{i=1}^{n+1} \exp(Y_i t^i) \pmod{t^{n+2}}.$$

Because the group H(Z) is complete, b follows. The unicity of the Y_i is evident from the construction.

3.2.2. Theorem (3.2.1) gives rise to the following corollaries:

Corollary 1. Let $G \in \mathrm{GCoalg}_k$ and let ϕ be a curve in G. Then there exists a unique family $(\xi_i)_{i\geq 1}$ in P(G) such that $\phi = \prod_{i=1}^{\infty} \exp(\xi_i t^i)$.

Proof. ϕ induces a continuous homomorphism $H(\phi) : H(Z) \to H(G)$ such that $H(\phi)(\Sigma Z_\mu t^\mu) = \phi$. The corollary follows by putting $\xi_i = \phi(Y_i)$.

For unicity observe that if $\prod_{i=1}^{\infty} \exp(\xi_i t^i) = \prod_{i=1}^{\infty} \exp(\eta_i t^i)$ and if $\xi_i = \eta_i$ for $1 \leq i \leq n$, one has $\prod_{n+1}^{\infty} \exp(\xi_i t^i) = \prod_{n+1}^{\infty} \exp(\eta_i t^i)$. Looking at the coefficients of t^{n+1} it follows $\xi_{n+1} = \eta_{n+1}$ and thus the family $(\xi_i)_{i \geq 1}$ is unique.

Corollary 2. Let $k[Y_i]$, $i \geq 1$ be copies of the bialgebra U of the additive group. Then $Z \simeq \coprod_{i=1}^{\infty} k[Y_i] = k\langle Y_1, Y_2, \ldots \rangle$ in GCoalg. $k\langle Y_1, Y_2, \ldots \rangle$ is the groupcoalgebra over k with diagonal d defined by $(Y_i)_{i \geq 1} \subset P(k\langle Y_i \rangle_{i \geq 1})$ and augmentation ε, $\varepsilon(Y_i) = 0$.

Proof. Observe that $\psi : P(G) \to \mathrm{GCoalg}\,(U,G)$, defined by $\psi(x) = \exp xt$ is a bijection, functorial in G. It follows from corollary 1 that

$$\mathrm{GCoalg}_k(Z,G) = H(G) \simeq \prod_{i \geq 1} (P(G))_i \simeq \prod_{i=1}^{\infty} \mathrm{GCoalg}\,(k[Y_i],G),$$

$(P(G))_i = P(G)$ for all i.

This means that Z represents the functor $\prod_{i=1}^{\infty} \mathrm{GCoalg}\,(k[Y_i],-)$ and thus $Z \simeq \coprod_{i=1}^{\infty} k[Y_i]$. Theorem (3.2.1a) shows that the Y_i are in fact free generators for Z as a k-algebra.

Corollary 3. Let B be a n-dimensional formal cogroup over k in the sense of Dieudonné, i.e. $B \simeq k[[t_1, \ldots, t_n]]$ as a k-algebra.
Let $U^{(n)} = \coprod_{i=1}^{n} k[Y_i]$ with the notations of corollary 2. Then there exists a surjection $\psi : U^{(n)} \to B^\vee$ in GCoalg_k.

Proof. Lie $B = P(B^\vee)$ is a n-dimensional k-vectorspace. Let $x_1, \ldots, x_n$ be a base for $P(B^\vee)$, then $\psi : U^{(n)} \to B^\vee$, $\psi(Y_i) = x_i$, $1 \leq i \leq n$ is the desired surjection. This is known from the structure theory of infinitesimal formal cogroups over a field k, $\chi(k) = 0$, because $B^\vee$ is the universal enveloping algebra of Lie B. In order to give the analogy with the case $\chi(k) = p > 0$ we sketch an alternative proof: Let $\exp x_i t = \Sigma x_{i\mu} t^\mu$ be the curves defined

by the x_i and take t_j as generators for B such that $\langle x_i, t_j \rangle = \delta_{ij}$. Calculating $r_{\mu,\nu} = \langle \overline{x}_{1\mu_1} \ldots \overline{x}_{n\mu_n}, t_1^{\nu_1} \ldots t_n^{\nu_n} \rangle$ with help of the Leibnizrelations one finds: $r_{\mu,\nu} = 0$ if $\Sigma\nu_i > \Sigma\mu_i$ and $\Sigma\nu_i = \Sigma\mu_i$ implies $r_{\mu,\nu} = \prod_{i=1}^{n} \delta_{\mu_i,\nu_i}$. It follows that the set of products $x_{1\mu_1} \ldots x_{n\mu_n}$ is a base for B^χ, thus ψ is surjective.

3§3 The decomposition theorem over a field k, $\chi(k) = p > 0$.

3.3.1. Theorem. (decomposition theorem in characteristic $p > 0$). Let Z be the UNG over $\mathbb{F}_p$. Then there exists a unique family $\{X_{ij}\}_{(i,j) \in S} \subset Z$, $S = \{(i,j) \in \mathbb{Z} \times \mathbb{Z} \mid i \geq 0,\ j \geq 1,\ (j,p) = 1\}$ such that:

a $X_{ij} = Z_{jp^i} + u_{ij}(Z_1, \ldots, Z_{jp^{i-1}})$ is isobaric.

b For each j the set $(X_{ij})_{i \geq 0}$ is E-pure, defining the curve

$$w_j = V_j(\Sigma E_\mu(X_{0j}, \ldots, X_{\mu j})t^\mu) = \Sigma E_\mu(X_{0j}, \ldots, X_{\mu j})t^{j\mu}.$$

c $\Sigma Z_\mu t^\mu = \prod_{(j,p)=1} w_j$ (natural order for j).

Corollary. The inclusion $Z \hookrightarrow k \otimes Z$ defines a canonical embedding $H(Z) \subset GCoalg_k(k \otimes Z, k \otimes Z) \underset{Def}{=} H_k(Z)$. Consequently, the canonical curve $\Sigma Z_\mu t^\mu \in H_k(Z)$ over an arbitrary field k, $\chi(k) = p > 0$ can be decomposed in a unique product of the curves w_j considered as elements of $H_k(Z)$.

Proof. The idea of the proof is the same as in (3.2.1). By the existence theorem we may consider the canonical E-pure curve $\Sigma E_\mu(X_0, \ldots, X_\mu)t^\mu$ as a curve in Z. Together with $X_0 = Z_1$ we thus have:

$$\Sigma Z_\mu t^\mu \equiv \Sigma E_\mu(X_0, \ldots, X_\mu)t^\mu \pmod{t^2}.$$

This leads to the induction hypothesis H''(n), $n \geq 1$:

There exist isobaric elements $X_{ij} = Z_{jp^i} + u_{ij}(Z_1, \ldots, Z_{jp^{i-1}})$ for all pairs $(i,j) \in S$ such that $jp^i \leq n$ and there exist E-pure sets $S_{j,n}$ for all $1 \leq j \leq n$, $(j,p) = 1$ such that P''(1) and P''(2) are true:

P''(1) Let s be the unique integer satisfying $jp^s \leq n < jp^{s+1}$, then $S_{j,n} = (X_{0j},\ldots,X_{sj},x^{(n)}_{s+1,j},\ldots)$. X_{ij} and $x^{(n)}_{ij}$ are isobaric of weight jp^i. $S_{j,n}$ defines the E-pure curve $v_{j,n}$. Put $w_{j,n} = V_j v_{j,n}$ and $D(n) = \prod_{\substack{\mu \leq n \\ (\mu,p)=1}} w_{\mu,n}$. (The order in the product is the natural order of the μ).

P''(2) $\Sigma Z_\mu t^\mu \equiv D(n) \pmod{t^{n+1}}$.

Observe that H''(1) is true, indeed: $S_{1,1} = (X_0,X_1,\ldots) = (X_{01},x^{(1)}_{11},x^{(1)}_{21},\ldots)$ and $X_{01} = X_0 = Z_1$. Thus let H''(n) be true for some $n \geq 1$. It follows from P''(1) that, writing $w_{j,n} = \Sigma x_\mu t^\mu$, x_μ is isobaric of weight μ. (Recall that the zero element has arbitrary weight). Because isobaricity behaves well under multiplication of curves it follows that the coefficient of t^μ in D(n) is isobaric of weight μ.

Let $D(n) = \Sigma D_\mu t^\mu$, then by assumption $D_\mu = Z_\mu$ if $0 \leq \mu \leq n$, thus $Z_{n+1} - D_{n+1} \in P(Z)$ and is isobaric of weight n+1. Consider the cases A and B:

Case A: $(n+1,p) = 1$. By (1.6.8) there exists a curve $\gamma = \Sigma \gamma_\mu t^\mu$ in Z such that $\gamma \equiv 1 + (Z_{n+1} - D_{n+1})t^{n+1} \pmod{t^{n+2}}$, γ_μ is isobaric of weight μ and $\gamma = V_{n+1}\bar{\gamma}$ for a unique curve $\bar{\gamma}$. The E-pure curve belonging to $\bar{\gamma}$ (2.3.1) is again isobaric and is defined by the E-pure set

$$S_{n+1,n+1} = (Z_{n+1} - D_{n+1},\ldots) = (X_{0,n+1},x^{(n+1)}_{1,n+1},\ldots).$$

The E-pure curve belonging to $\bar{\gamma}$ will be denoted by $v_{n+1,n+1}$ and $w_{n+1,n+1} = V_{n+1} v_{n+1,n+1}$. In order to satisfy P''(1) of H''(n+1) we merely change the notations: Put $S_{j,n+1} = S_{j,n}$, $x^{(n+1)}_{m,j} = x^{(n)}_{m,j}$ and $w_{j,n+1} = w_{j,n}$ for $1 \leq j \leq n$.

The sets $S_{j,n+1}$ completed with $S_{n+1,n+1}$ satisfies P''(1) of H''(n+1).

For P''(2) we have:

$$D(n+1) \underset{\text{Def}}{=} D(n)w_{n+1,n+1} = \prod_{\substack{\mu \le n+1 \\ (\mu,p)=1}} w_{\mu,n+1} \quad \text{(ordered by } \mu\text{)}$$

$$\equiv (1 + Z_1 t + \ldots + Z_n t^n + D_{n+1} t^{n+1})(1 + (Z_{n+1} - D_{n+1}) t^{n+1}) \pmod{t^{n+2}}$$

$$\equiv \Sigma Z_\mu t^\mu \pmod{t^{n+2}}.$$

Remains the verification that $X_{0,n+1} = Z_{n+1} - D_{n+1} = Z_{n+1} + u_{0,n+1}(Z_1,\ldots,Z_n)$. We assert that D_{n+1} does not have a term Z_{n+1}. Consider the canonical E-pure curve $\Sigma E_\mu(X_0,\ldots,X_\mu)t^\mu$. The coefficients of t^μ, $1 \le \mu \le p^{s+1} - 1$ are isobaric polynomials in $X_0,\ldots,X_s$. Taking the curve $V_j \Sigma E_\mu t^\mu$ we have: the coefficients of t^μ in this curve such that $1 \le \mu \le j(p^{s+1} - 1) + (j - 1) = jp^{s+1} - 1$ are isobaric polynomials in $X_0,\ldots,X_s$ or are zero. (The term (j-1) is due to these zeros). Applying this to the curve $w_{j,n+1}$ we have by P''(1): $jp^s \le n < jp^{s+1}$. In our case A we have even $n+1 < jp^{s+1}$, i.e. $n+1 \le jp^{s+1} - 1$ and by the foregoing it thus follows that the coefficient of t^{n+1} in $w_{j,n+1}$ is an isobaric polynomial in $X_{0,j},\ldots,X_{s,j}$. Because all pairs (i,j) involved satisfy $jp^i \le n$ we thus have $D_{n+1} \in \mathbb{F}_p\langle Z_1,\ldots,Z_n\rangle$ as claimed. Thus H''(n+1) is true in case A.

Case B: $(n+1,p) = p$. Let j be such that $(j,p) = 1$, $jp^{s+1} = n+1$ and consider $S_{j,n} = (X_{0j},\ldots,X_{sj}, x^{(n)}_{s+1,j},\ldots)$. The coefficient of t^{n+1} in $w_{j,n}$ defined by $S_{j,n}$ is $x^{(n)}_{s+1,j}$. Thus by (1.5.3) we have:

$$Vx^{(n)}_{s+1,j} = X_{s,j} = Z_{jp^s} + u_{s,j}(Z_1,\ldots,Z_{jp^{s-1}}), \text{ thus}$$

$$x^{(n)}_{s+1,j} \equiv Z_{jp^{s+1}} + u_{s,j}(Z_p,\ldots,Z_{jp^{s+1}-p}) \mod \operatorname{Ker} V.$$

By isobaricity and the fact $Z_\mu \in \operatorname{Ker} V$ iff $(\mu,p) = 1$ we find

$$x^{(n)}_{s+1,j} = Z_{jp^{s+1}} + \xi(Z_1,\ldots,Z_n). \tag{3.2}$$

By the arguments of case A we have: no $w_{\mu,n}$, $\mu \neq j$ contains as coefficient of t^{n+1} a term involving $Z_{jp^{s+1}} = Z_{n+1}$, i.e. the coefficient D_{n+1} has in

case B the form:

$$D_{n+1} = Z_{n+1} + g(Z_1,\ldots,Z_n). \tag{3.3}$$

Because $D_\mu = Z_\mu$, $0 \leq \mu \leq n$, $D_{n+1} - Z_{n+1} = g(Z_1,\ldots,Z_n) \in P(Z)$. By (1.6.8) we can find a curve $\gamma = \Sigma\gamma_\mu t^\mu$ in Z such that $\gamma \equiv 1+(Z_{n+1}-D_{n+1})t^{n+1} \pmod{t^{n+2}}$, and γ_μ is isobaric of weight μ. Let $v_{j,n+1}$ be the E-pure curve belonging to the productcurve $v_{j,n}\cdot\gamma$, then $v_{j,n+1}$ is defined by the E-pure set

$$\begin{aligned} S_{j,n+1} &= (X_{0j},\ldots,X_{sj},\ x^{(n)}_{s+1,j} + Z_{n+1} - D_{n+1},\ldots) \\ &= (X_{0j},\ldots,X_{sj},\ X_{s+1,j},\ x^{(n+1)}_{s+2,j},\ldots) \end{aligned}$$

and every element of $S_{j,n+1}$ is isobaric.

Further:

$$\begin{aligned} X_{s+1,j} &= x^{(n)}_{s+1,j} + Z_{n+1} - D_{n+1} \\ &= Z_{jp^{s+1}} + f(Z_1,\ldots,Z_n) - g(Z_1,\ldots,Z_n) = \qquad \text{(3.2) and (3.3)} \\ &= Z_{jp^{s+1}} + u_{s+1,j}(Z_1,\ldots,Z_n). \end{aligned}$$

We can now satisfy P''(1) of H''(n+1) by changing the notations as in case A: $S_{\mu,n+1} = S_{\mu,n}$, $\mu \neq j$, $x^{(n+1)}_{i,\mu} = x^{(n)}_{i,\mu}$.

Put $w_{j,n+1} = V_j v_{j,n+1}$ and $w_{\mu,n+1} = w_{\mu,n}$ if $\mu \neq j$.

We claim: $D(n+1) = \prod\limits_{\substack{\mu\leq n+1 \\ (\mu,p)=1}} w_{\mu,n+1} = \Sigma Z_\mu t^\mu \pmod{t^{n+2}}$.

Indeed: $w_{j,n+1} \equiv w_{j,n}\cdot(1 + (Z_{n+1} - D_{n+1})t^{n+1}) \bmod (t^{n+2})$.

$$D(n+1) = \prod_{\substack{\mu<j \\ (\mu,p)=1}} w_{\mu,n} \cdot w_{j,n}\cdot(1 + (Z_{n+1} - D_{n+1})t^{n+1}) \prod_{\substack{\mu\leq n+1 \\ (\mu,p)=1 \\ \mu>j}} w_{\mu,n} \pmod{t^{n+2}}$$

Observe that $1 + (Z_{n+1} - D_{n+1})t^{n+1}$ commutes with every $w_{\mu,n} \pmod{t^{n+2}}$, thus:

$$\begin{aligned} D(n+1) &\equiv D(n)\ (1 + (Z_{n+1} - D_{n+1})t^{n+1}) \pmod{t^{n+2}} \\ &\equiv (1 + Z_1 t + \ldots + Z_n t^n + D_{n+1}t^{n+1})(1 + (Z_{n+1} - D_{n+1})t^{n+1}) \pmod{t^{n+2}} \\ &\equiv \Sigma Z_\mu t^\mu \pmod{t^{n+2}} \end{aligned}$$

Hence H''(n+1) is true in case B.

In view of the topology of H(Z) the sequence of curves $w_{j,n}$ converges to a limit curve w_j, and as in obvious:

$$\Sigma Z_\mu t^\mu = \lim_{n\to\infty} \prod_{(j,p)=1}^{n} w_j = \prod_{(j,p)=1}^{\infty} w_j .$$

Denoting Z' the $\mathrm{UNG}_{\mathbf{F}_p}$ and $Z = k \otimes Z'$ the UNG_k, we have $Z' \hookrightarrow Z$ and $H(Z') \subset H(Z)$ in a natural way. The proof shows that the decomposition of $\Sigma Z_\mu t^\mu$ can already be carried out in the subgroup H(Z') and the X_{ij} are obviously unique. This proves theorem (3.3.1) and the Corollary.

3.3.2. As in the characteristic zero case, theorem (3.3.1) gives rise to the following corollaries:

Corollary 1. Let $\chi(k) = p > 0$, $G \in \mathrm{GCoalg}_k$ and let ϕ be a curve in G. Then there exists a unique family $\{\xi_{ij}\}_{ij \in S} \subset G$ such that the $(\xi_{ij})_{i\geq 0}$ define for every j the E-pure curve v_j and such that $\phi = \prod_{(j,p)=1}^{\infty} V_j v_j$ (natural order for j).

Proof. Consider the continuous homomorphism $H(\phi) : H(Z) \to H(G)$ and put $\phi X_{ij} = \xi_{ij}$. For the unicity first observe that it follows from the decomposition theorem a, that the Z_μ can be expressed in terms of the X_{ij}, say $Z_{jp^i} = X_{ij} + d_{ij}(X_{ab})$. The d_{ij} are universal polynomials in the X_{ab}, satisfying $bp^a < jp^i$. It follows that if $\phi = \Sigma \phi_\mu t^\mu$, we have $\phi_{jp^i} = \xi_{ij} + d_{ij}(\xi_{ab})$. Moreover if $\{\eta_{ij}\}_{ij \in S}$ is a second set of elements of G, satisfying the conditions of the corollary, we necessarily have $\phi_{jp^i} = \eta_{ij} + d_{ij}(\eta_{ab})$. By recurrency it follows that $\eta_{ij} = \xi_{ij}$ for all $(i,j) \in S$.

Corollary 2. Let $k\langle X_{ij}\rangle_{i\geq 0}$ for every j, (j,p) = 1, be a copy of the NEG_k over k, such that the set $(X_{ij})_{i\geq 0}$ is E-pure. Then:

$$Z \underset{\sim}{} \coprod_{(j,p)=1} k\langle X_{ij}\rangle_{i\geq 0} \underset{\sim}{} k\langle X_{ij}\rangle_{(i,j)\in S} \quad \text{in } \mathrm{GCoalg}_k.$$

The diagonal d is given by the condition: the set $(X_{ij})_{i\geq 0}$ is E-pure for every j and $\varepsilon(X_{ij}) = 0$.

Proof. Observe that there exists a canonical functorial bijection between the set of E-pure curves in G and GCoalg (U,G). It follows from corollary 1 that $\mathrm{GCoalg}_k(Z,G) = H(G) \underset{\sim}{} \coprod_{(j,p)=1} \mathrm{GCoalg}\ (U,G)_j$.
$\mathrm{GCoalg}\ (U,G)_j = \mathrm{GCoalg}\ (U,G)$ for every j.
The corollary then is evident and theorem (3.3.1) shows that the X_{ij} are free generators for Z.

Corollary 3. Let $\chi(k) = p > 0$ and let B be a n-dimensional formal cogroup over k in the sense of Dieudonné, i.e. $B \underset{\sim}{} k[[t_1,\ldots,t_n]]$ as a k-algebra. Let $U^{(n)} = k\langle X_{ij}\rangle_{i\geq 0,\ 1\leq j\leq n}$ be the direct sum of n copies of U in GCoalg_k, such that the sets $(X_{ij})_{i\geq 0}$ are E-pure. Then there exists a surjective morphism $\psi : U^{(n)} \to B$ in GCoalg_k and the set $\{\psi X_{ij}\}_{i,j}$ defines an ordered p-base of E-pure semiderivations in B^*.

Proof. Consider curves in B^* as elements of $\mathrm{Al}_k\ (B,k[[t]])$. One then has the curves $\phi_i : B \to k[[t]]$, $\phi_i(t_j) = \delta_{ij}t$, $1 \leq i,j \leq n$. Let $\phi_i = \Sigma\phi_{i\mu}t^\mu$ then the $q_{ij} = \phi_{ipj}$ define an ordered p-base for B^* (Corollary 1(1.6.6).) Let ψ_i be the E-pure curve belonging to ϕ_i, defined by the E-pure set $(\xi_{ij})_{i\geq 0} \subset B^*$. In view of $V\xi_{ij} = \xi_{i-1,j}$ it follows that the set $(\xi_{ij})_{i\geq 0,\ 1\leq j\leq n}$ defines an ordered p-base for B^*.
Indeed: $\overline{\xi}_{ij}$ is $F^{i+1}B$-linear on B and is a F^ik-derivation of F^iB (lemma 1.5.6). The ξ_{oj}, $1 \leq j \leq n$ form a base for $P(B^*)$ and we can apply the reasoning of 1.6.5b (cf. too 1.6.6 corollary 2).

Corollary 4. Let with the notations of corollary 3, $x \in \mathrm{Lie}\ B = P(B^*)$, then there exists an E-pure curve $\Sigma E_\mu(\xi_0,\ldots,\xi_\mu)t^\mu$ in B^* such that $\xi_0 = x$.

Proof. Let $I = \mathrm{Ker}\{\varepsilon : B \to k\}$, then $P(B^{\chi}) \tilde{=} (I/I^2)^{*}$. Take a base $x=x_1,x_2,\ldots,x_n$ for $P(B^{\chi})$ and let $t_1,\ldots,t_n \in B$ be pointdistributions on the x_i, $1 \leq i \leq n$, such that $\langle t_1,x_1\rangle = 1$. Then $B = k[[t_1,\ldots,t_n]]$. Take the curve ψ_1 of the proof of corollary 3.

Corollary 4 answers to a question of J. Dieudonné. [4, 13 page 443].

3.3.3. The fact that the exponential groupcoalgebra U over a field k, $\chi(k) = p > 0$ is bigger than the bialgebra of the additive group, gives rise to the phenomenon of the existence of groups of finite height. It results from (3.1.2) and the decomposition theorem that there exist no non trivial curves of infinite lenghth in the subgroupcoalgebras $U(r) = k\langle X_0,\ldots,X_r\rangle$ if $r < \infty$. Now consider finite curves ϕ in $G \in \mathrm{GCoalg}_k$, i.e. morphisms $Z(r) \to G$. If $\chi(k) = 0$ the decomposition theorem gives that $\phi = \sum_{\mu}^{r} \phi_\mu t^\mu = \prod_{i=1}^{r} \exp(\xi_i t^i) \pmod{t^{r+1}}$ for unique $\xi_i \in P(G)$. In particular every finite curve then can be prolonged to an infinite curve. The same is not longer true if $\chi(k) = p > 0$. One has obviously $Z(r) \tilde{=} k\langle X_{ij}\rangle$ where the i,j satisfy: $i \geq 0$, $j \geq 1$, $(j,p) = 1$, $jp^i \leq r$ and if j is constant, the $(X_{ij})_{i\geq 0}$ define finite E-pure sets. The decomposition theorem gives: If $G \in \mathrm{GCoalg}_k$ and $\phi = \sum_{\mu}^{r} \phi_\mu t^\mu$ is a finite curve in G, then there exists a unique family $\{\xi_{ij}\}_{i,j} \subset G$, such that $(j,p) = 1$, $jp^i \leq r$ and such that $(\xi_{ij})_{i\geq 0}$ defines a finite E-pure curve v_j, and then $\phi = \prod_{(j,p)=1} V^j v_j \pmod{t^{r+1}}$.

It is clear that in general the curves v_j cannot be extended to infinite curves. In view of the relation $\langle 0,f\rangle = \langle V^{r+1}X_j,f\rangle^{p^{r+1}} = \langle X_j,f^{p^{r+1}}\rangle = 0$ if $X_j \in U(\underline{r})$ and $f \in U(\underline{r})^{*}$ we see that $U(\underline{r})^{\chi}$ has height $\leq r+1$.

Corollary 3 now has a "finite height"-analogon which may be useful in a structure theory of a certain class of formal cogroups.

3.3.4. Proposition. Let $\chi(k) = p > 0$ and let $\bar{k}$ be a perfect closure of k. Let $B \in \mathrm{CAl}_k$ be such that $\bar{B} = \bar{k} \otimes_k B$ has height $\leq r+1$. Let $(\xi_i)_{i\in S}$ be a

base for Lie $B = P(B^*)$ and $U(r)^{(S)}$ be a direct sum in $GCoalg_k$ of copies of $U(r)$. Then there exists a surjective morphism $\psi : U(r)^{(S)} \to B^*$ in $GCoalg_k$.

Proof. By the Dieudonné-Cartier theorem (1.3.9) we have: $\overline{B} \simeq \overline{k}[[t_i]]/(t_i^{p^{n_i+1}})_{i \in T}$ where T is suitable index set for the indeterminates t_i. Assuming that the t_i are independent generators for $\overline{B}$ over $\overline{k}$, we may identify T and S. Moreover we may assume that $t_i \in B \subset \overline{B}$. Consider the curve $\psi_i \in Al_{\overline{k}}(\overline{B},\overline{k}[[t]]/(t^{p^{n_i+1}})) \simeq Al_k(B,\overline{k}[[t]]/(t^{p^{n_i+1}}))$, defined by $\psi_i(t_j) = \delta_{ij}t$, then $\psi_i = \Sigma\psi_{i\mu}t^\mu$ where the $\psi_{i\mu}$ are $\overline{k}$-linear maps $\psi_{i\mu} : \overline{B} \to \overline{k}$ satisfying $\psi_{i\mu}(uv) = \sum_{\rho+\sigma=\mu} \psi_{i\rho}(u)\,\psi_{i\sigma}(v)$.
Now observe that the $\psi_{i\mu}$ are pointdistributions on the powers t_i^μ and are zero on every other monomial in the t_j. It thus follows that not only the restriction of $\psi_{i\mu}$ to B is a k-linear map $B \to \overline{k}$, but even a k-linear map $B \to k$, i.e. we can view $\psi_{i\mu}$ as elements of B^χ. With a slight obvious generalisation of corollary 1, (1.6.6) we have, putting $q_{ij} = \psi_{ip^j}$, that the set of all q_{ij}, $i \in T$, $0 \le j \le n_i$ defines an ordered p-base for B^χ. Let ϕ_i be the E-pure curve belonging to ψ_i, (2.3.1), defined by the E-pure set (ξ_{ij}), $0 \le j \le n_i$. Because the process of taking E-pure curves belonging to given curves is defined over the prime field, we conclude $\xi_{ij} \in B^\chi$ and moreover: all ξ_{ij} define an ordered p-base for B^*. One can see this by considering the expressions $\xi_{ij} = q_{ij} + u_j(\psi_{i1},\dots,\psi_{i,p^{j-1}})$ (existence theorem 2.1.4a): The q_{ij} are modified by elements that are zero on F^jB, i.e. the restrictions of ξ_{ij} and q_{ij} to F^jB coincide.
We thus now have E-pure sets $(\xi_{i0},\xi_{i1},\dots,\xi_{i,n_i})$ in B^*. Consider the canonical E-pure curve $E = \Sigma E_\mu(X_0,\dots,X_\mu)t^\mu$. Then

$$\begin{aligned}
\Sigma V(E_\mu(X_0,\dots,X_\mu))t^\mu &= \Sigma E_\mu(0,X_0,\dots,X_{\mu-1})t^\mu && \text{(a)}\\
&= \Sigma E_{\frac{\mu}{p}}(X_0,\dots,X_{\mu-1})t^\mu && (E_{\frac{\mu}{p}} = 0 \text{ if } (\mu,p) = 1)\\
&= \Sigma E_\nu(X_0,\dots,X_\nu)t^{\nu p}\\
&= V_pE && \text{(b)}
\end{aligned}$$

thus in particular, comparing (a) and (b), V_pE is again an E-pure curve defined by the E-pure set $(0,X_0,X_1,\ldots)$. It follows: if $(\eta_0,\ldots,\eta_n)$ is an E-pure set then $(0,\eta_0,\ldots,\eta_n)$ is an E-pure set.

Applying this to the E-pure sets $(\xi_{i0},\ldots,\xi_{i,n_i})$ we have the E-pure sets $(\underbrace{0,\ldots,0}_{r-n_i \text{ times}},\xi_{i,0},\ldots,\xi_{i,n_i}) = (\eta_{i0},\ldots,\eta_{i,r})$. Putting $U(r)^{(S)} = k\langle X_{ij}\rangle_{i\in S,\ 0\leq j\leq r}$, such that the $(X_{ij})_j$ are E-pure for each $i \in S$, the morphism $\psi : U(r)^{(S)} \to B^*$, defined by $\psi(X_{ij}) = \eta_{ij}$ satisfies the conditions of the propositions.

3§4 E-pure sets.

3.4.1. Notation. Let k be an arbitrary field, $\chi(k) = p > 0$. We put $L(G) = GCoalg_k(U,G)$ and $L_n(G) = GCoalg_k(U(n),G)$ for $G \in GCoalg_k$. $U(n) = k\langle X_0,\ldots,X_n\rangle$ is the subgroupcoalgebra of the NEG_k. $U = k\langle X_i\rangle_{i\geq 0}$. $(X_i)_{i\geq 0}$ is the canonical E-pure set. Observe that E-pure curves and E-pure sets define each other unambiguously, and that we can identify L(G) with the set of all E-pure sets in G, or with the set of all infinite E-pure curves in G. A finite analogonof this obviously holds for $L_n(G)$.

3.4.2a. As is evident, $U \perp\!\!\!\perp U = k\langle X_i,Y_i\rangle_{i\geq 0}$. Let the sets $X = (X_i)_{i\geq 0}$ and $Y = (Y_i)_{i\geq 0}$ be E-pure, defining the E-pure curves E(X) and E(Y). Applying the decomposition theorem (3.3.1) to the productcurve E(X)E(Y) in the group $H(U \perp\!\!\!\perp U)$ we have $E(X)E(Y) = \prod_{(j,p)=1} w_j$ where the w_j are defined by E-pure sets. In particular let w_1 be defined by the E-pure set $X \times Y = ((X \times Y)_i)_{i\geq 0}$ in $U \perp\!\!\!\perp U$. Then the morphism $U \to U \perp\!\!\!\perp U$ in $GCoalg_k$, defined by $X_i \longmapsto (X \times Y)_i$, $i \geq 0$, defines a law of composition, denoted $\times$,

$$\times : L(U) \times L(U) \to L(U)$$

and by functoriality, a law of composition, again denoted $\times$,

$$\star : L(G) \times L(G) \to L(G).$$

Note however that $\star$ is in general not associative. Giving X_i and Y_i the weight p^i and observing that $E(X)E(Y)$ is an isobaric curve, one easily checks that

$$(3.4) \qquad (X \star Y)_i = X_i + Y_i + g_i(X_{i-1},\dots,X_0,Y_{i-1},\dots,Y_0),$$

where g_i is isobaric and defined over $\mathbb{F}_p$.
Notice that for the E-pure set $(\eta_i)_{i\geq 0}$ we have $V\eta_i = \eta_{i-1}$ (2.3.1), hence $V^i\eta_i = \eta_0$. Observing that $(X \star Y)_0 = X_0 + Y_0$, one sees that $X_i + Y_i$ must occur in (3.4). Specialisation of the E-pure set $(Y_i)_{i\geq 0}$ to the E-pure set $(0,0,\dots,0,\dots)$ gives: $g_i(X_{i-1},\dots,X_0,0,\dots,0) = 0$.
Let $G \in Ab_k$, then $L(G) = GCoalg_k(U,G) \simeq Ab_k(A,G)$ is an abelian group, functorial in G, (3.1.7). It follows easily that $\star : L(G) \times L(G) \to L(G)$ defines in this case the grouplaw on L(G).

3.4.2b. Let E(X) be the canonical E-pure curve in U. Then applying the decomposition theorem to the curve $E(X)^{-1} = \prod_{(j,p)} w_j$, one finds that w_1 is defined by an E-pure set, denoted $((cX)_i)_{i\geq 0}$. The morphism $c : U \to U$ in $GCoalg_k$, defined by $c(X_i) = (cX)_i$, $i \geq 0$, defines an endomorphism $c : L(U) \to L(U)$, and by functoriality an endomorphism $c : L(G) \to L(G)$. By isobaricity we have:

$$(3.5) \qquad (cX)_i = -X_i + h_i(X_{i-1},\dots,X_0)$$

and h_i is isobaric of weight p^i, defined over $\mathbb{F}_p$.

In the commutative case, i.e. if $G \in Ab_k$, one verifies easily, using (3.1.7) that $c : L(G) \to L(G)$ is the inversion morphism for the abelian group L(G).

3.4.2c. With the notations of (3.4.2b) let $\prod_{(j,p)=1} w_j$ be the decomposition

of the curve $E(X)^p = \Sigma\gamma_\mu t^\mu$. Because $\gamma_\mu = \sum_{\mu_1+\ldots+\mu_p=p} E_{\mu_1}\ldots E_{\mu_p}$, one has: $\gamma_\mu = 0$ if $1 \leq \mu < p$ and $\gamma_p = X_0^p$. Indeed, the E_μ commute if $1 \leq \mu < p$ and the number of solutions of $\mu_1+\ldots+\mu_p = p$ is a multiple of p except when all $\mu_i = 1$. It follows that w_1 is defined by an E-pure set having the form $(0,X_0^p,u_2,u_3,\ldots)$. In view of the lemma below, $(X_0^p,u_2,u_3,\ldots)$ is again an E-pure set, denoted $((FX)_i)_{i\geq 0}$.
In view of $V^i(FX)_i = (FX)_0 = X_0^p$, one sees that

$$(3.6) \qquad (FX)_i = X_i^p + f_i(X_{i-1},\ldots,X_0),\ i \geq 0$$

where the f_i are isobaric polynomials, defined over $\mathbb{F}_p$.
By functoriality, the morphism $F : U \to U$ in $GCoalg_k$, defined by $F(X_i) = (FX)_i$, $i \geq 0$, defines an endomorphism, denoted F,

$$F : L(G) \to L(G),$$

functorial in G.
In the commutative case, $E(X)^p$ is again E-pure, and an easy calculation shows that $(FX)_i = X_i^p$ and that $F : L(G) \to L(G)$ is a groupendomorphism of the abelian group L(G), functorial in $G \in Ab_k$.

3.4.2d. Lemma. Let $G \in GCoalg_k$. Then the set $(\xi_i)_{i\geq 0}$ in G is E-pure iff the set $(V\xi_i)_{i\geq 0} = (0,\xi_0,\xi_1,\ldots)$ is E-pure. In particular the map $(\xi_i)_{i\geq 0} \longmapsto (V\xi_i)_{i\geq 0}$ defines an endomorphism $V : L(G) \to L(G)$, functorial in G.

Proof. We must show that $d\xi_i = \sum_{\mu+\nu=p^i} E_\mu(\xi_0,\ldots,\xi_\mu) \otimes E_\nu(\xi_0,\ldots,\xi_\nu)$ for all i iff $d\xi_i = \sum_{\mu+\nu=p^{i+1}} E_\mu(0,\xi_0,\ldots,\xi_{\mu-1}) \otimes E_\nu(0,\xi_0,\ldots,\xi_{\nu-1})$ for all i.
This follows easily from the relations:

$$\begin{aligned} E_\mu(0,\xi_0,\ldots,\xi_{\mu-1}) &= E_\mu(V\xi_0,\ldots,V\xi_\mu) && \text{(by 1.5.3)} \\ &= VE_\mu(\xi_0,\ldots,\xi_\mu) && (E_\mu \text{ is rational over } \mathbb{F}_p) \\ &= E_{\frac{\mu}{p}}(\xi_0,\ldots,\xi_{\mu-1}) && \text{(by 1.5.3 again).} \end{aligned}$$

Here we put $E_{\frac{\mu}{p}} = 0$ if $(\mu,p) = 1$. The lemma then is straightforward.

Notice that in the commutative case $V : L(G) \to L(G)$ is a groupendomorphism of the abelian group $L(G)$, functorial in $G \in Ab_k$.

3.4.2e. With the notations of (3.4.2a) consider the curve $E(X)E(Y)E(X)^{-1}E(Y)^{-1} = \prod_{(j,r)} w_j^j$. The curve w_2 is defined by an E-pure set, denoted $((X,Y)_i)_{i\geq 0}$.
Taking the finite E-pure curves $1 + X_0t + X_1t$ if $p = 2$ and $1 + X_0t + \frac{1}{2}X_0^2t^2$ if $p \neq 2$ ($E_2 = \frac{1}{2}X_0^2$ in view of (3.1.4) and isobaricity), one obtains:

$$(X,Y)_0 = X_0Y_0 + Y_0X_0 + X_0^2 + Y_0^2 \quad \text{if } p = 2$$
$$= X_0Y_0 - Y_0X_0 \quad \text{if } p \neq 2.$$

In view of $V^i(X,Y)_i = (X,Y)_0$ and isobaricity one concludes that

$$(3.7) \qquad (X,Y)_i = X_iY_i - Y_iX_i + c_i(X_i,\ldots,X_0,Y_i,\ldots,Y_0)$$

where the c_i are isobaric polynomials, rational over $\mathbb{F}_p$, such that c_i does not contain any term X_iY_i or Y_iX_i. The morphism $(\ ,\ ) : U \to U \amalg U$ in $GCoalg_k$, $(\ ,\ )(X_i) = (X,Y)_i$ induces a map,

$$(\ ,\ ) : L(G) \to L(G),$$

functorial in G.

In the commutative case, $(\ ,\ )$ is the zero homomorphism.

3.4.2f. If $\lambda \in k$ and $E(X)$ is the canonical E-pure curve, then the curve $\lambda \times E(X)$ (1.4.9c) is again E-pure and is defined by the E-pure set $(\lambda^{p^i}X_i)_{i\geq 0}$. This induces an operation

$$(3.8) \qquad k \times L(G) \to L(G),\ (\lambda,x) \longmapsto \lambda * x,$$

functorial in G.

In the commutative case, (1.4.9c) shows that $\lambda^* : L(G) \to L(G)$ is a groupendomorphism of the abelian group $L(G)$, functorial in $G \in Ab_k$. $F\lambda = \lambda^p F$ and $V\lambda^p = \lambda V$.

3.4.3. It is obvious that the operations $*$, F, V, c, (,) and the operations of k induce analoguous operations on the finite E-pure sets in G, and that the natural inclusion $U(n) \hookrightarrow U$ in $GCoalg_k$ induces a map, denoted $\rho_n : L(U) \to L_n(U)$, compatible with all the operations defined in (3.4.2). By functoriality one has a map $\rho_n : L(G) \to L_n(G)$, functorial in $G \in GCoalg_k$. Consider in particular the set $L_0(G) = GCoalg_k(U(0),G) = \{x \in G \mid dx = x \otimes 1 + 1 \otimes x\} = P(G)$. The next lemma is now easily verified.

3.4.4. Lemma. Let $p \neq 2$, then the operations of (3.4.2) define on $L_0(G) = P(G)$ the structure of a p-Liealgebra over k, and this p-Liealgebra structure is the same as the usual p-Liealgebra of the formal cogroup G^*.

3.4.5. It can also easily be verified that the following relations hold: $FV = VF$, and $V\lambda = \lambda^{1/p}V$. Note that $\lambda^{1/p}V$ has a sense even if $\lambda^{1/p} \notin k$. Other possible relations between the operations $*$, c, F, V, (,) and $\lambda*$ are still obscure in the non commutative case. We shall see however in 4§1 that nevertheless these operations give precise information about the structure of the Cartieduals of infinitesimal formal cogroups.

3.4.6. Let $(X_i)_{i\geq 0}$ be the canonical E-pure set. By lemma (3.4.2d) the set $(VX_i)_{i\geq 0}$ is again E-pure and defines the endomorphism T of U in $GCoalg_k$, $T(X_i) = X_{i-1}$, $i \geq 0$, $X_{-1} \underset{\text{Def}}{=} 0$. The induced map, again denoted $T : U(n+1) \to U(n)$, $T(X_i) = X_{i-1}$, $0 \leq i \leq n+1$ induces an injection, equally denoted $T : L_n(G) \hookrightarrow L_{n+1}(G)$, functorial in G; $T(X_0,\ldots,X_n) = (0,X_0,\ldots,X_n)$. One easily checks the following properties of T: T commutes with $*$, F, V, c and (,). $T\lambda = \lambda^{1/p}T$, $\lambda \in k$.

3§5 Campbell-Hausdorff structures.

As in 3§2 we first sketch the situation over a groundfield k, $\chi(k) = 0$.

3.5.1. Let $Z = k\langle X_1, X_2, \ldots\rangle$ be the UNG over k, $\chi(k) = 0$, $dX_i = X_i \otimes 1 + 1 \otimes X_i$ (3.2.2. cor 2). Now if $x \in P(Z)$, then $\exp xt = \sum_{i=0}^{\infty} \frac{x^i t^i}{i!}$ is a curve in Z, thus in particular

$$F_n = \exp (X_1 + X_2 + \ldots + X_n)t = \Sigma F_{n,\mu} t^{\mu}$$

is a curve in Z.

Attaching to each X_i the weight $\omega(X_i) = i$ (3.2.1. th.a), $F_{n,\mu}$ is not isobaric of weight μ. Put $F_{n,\mu} = \sum_{\rho=0}^{\infty} F_{n,\mu,\rho}$ as a unique sum of isobaric parts, $\omega(F_{n,\mu,\rho}) = \rho$. This sum is in fact finite.

Collecting isobaric parts, we form a new sum

$$G^{(n)} = \sum_{\rho=0}^{\infty} \Big(\sum_{\mu=0}^{\infty} F_{n,\mu,\rho} \Big) t^{\rho} = \sum_{\rho=0}^{\infty} G_{\rho}^{(n)} t^{\rho}.$$

Notice that $G_{\rho}^{(n)}$ is a finite sum, for $F_{n,\mu,\rho} = 0$ if $\mu > \rho$.

Lemma 1. $G^{(n)}$ is a curve in Z.

Proof. We have to verify that $G_0^{(n)} = 1$ (trivial) and that $dG_{\rho}^{(n)} = \sum_{\alpha+\beta=\rho} G_{\alpha}^{(n)} \otimes G_{\beta}^{(n)}$. Because F_n is a curve, we have:

$$dF_{n,\mu} = \sum_{a+b=\mu} F_{n,a} \otimes F_{n,b}$$

thus

$$\sum_{\rho=0}^{\infty} dF_{n,\mu,\rho} = \sum_{a+b=\mu} \sum_{\alpha=0}^{\infty} \sum_{\beta=0}^{\infty} F_{n,a,\alpha} \otimes F_{n,b,\beta}.$$

Now observe that d is compatible with the weight function ω, if we take the total weight on $Z \otimes Z$, in view of $dX_i = X_i \otimes 1 + 1 \otimes X_i$.

It follows that $dF_{n,\mu,\rho}$ must be the isobaric part of total weight ρ in the right hand side, i.e.:

$$dF_{n,\mu,\rho} = \sum_{a+b=\mu} \sum_{\alpha+\beta=\rho} F_{n,a,\alpha} \otimes F_{n,b,\beta} \quad , \text{ hence}$$

$$dG_{\rho}^{(n)} = \sum_{\mu=0}^{\infty} dF_{n,\mu,\rho} = \sum_{\mu=0}^{\infty} \sum_{a+b=\mu} \sum_{\alpha+\beta=\rho} F_{n,a,\alpha} \otimes F_{n,b,\beta}$$

$$= \sum_{a=0}^{\infty} \sum_{b=0}^{\infty} \sum_{\alpha+\beta=\rho} F_{n,a,\alpha} \otimes F_{n,b,\beta}$$

$$= \sum_{\alpha+\beta=\rho} G_{\alpha}^{(n)} \otimes G_{\beta}^{(n)}.$$

There is no difficulty in interchanging the orders of summation because every sum is a finite sum.

If more general $u \in Z[[t]]$ and $u \equiv 0 \pmod{t}$, then $\exp u \underset{\text{def}}{=} \sum_{i=0}^{\infty} \frac{u^i}{i!}$ is a well defined element of $Z[[t]]$. From the construction it now follows:

Corollary. $G^{(n)} = \exp(X_1 t + \ldots + X_n t^n)$, considered as a formal powerseries in t, is a curve in Z.

Lemma 2. $G^{(n)} \equiv G^{(n+1)} \pmod{t^{n+1}}$.

Proof. Considering $(X_1 t + \ldots + X_{n+1} t^{n+1})^{\mu}$ one sees that every monomial in $X_1, \ldots, X_n$, occurring in $G^{(n+1)}$ occurs in $G^{(n)}$ as well. If X_{n+1} occurs, it is at least in the coefficient of t^{n+1}.

Because $H(Z)$ is a complete topological group, we see that

$$(3.9) \qquad G = \Sigma G_{\mu} t^{\mu} = \lim_{n\to\infty} G^{(n)} = \exp\left(\sum_{i=1}^{\infty} X_i t^i\right)$$

is a curve in Z. Each G_{μ} is isobaric of weight μ and

$$(3.10) \qquad G_{\mu} = X_{\mu} + f_{\mu}(X_{\mu-1}, \ldots, X_1)$$

where f_{μ} is isobaric of weight μ, $\mu \geq 1$.

Consider the composite map $Z \xrightarrow{G} Z \xrightarrow{G^{-1}} Z$ in $GCoalg_k$, defined by $G(Z_{\mu}) = G_{\mu}$. In view of (3.10), G is an automorphism, hence G^{-1} is defined in $GCoalg_k$.

It follows:

$$(3.11)\quad \Sigma Z_\mu t^\mu = G^{-1} \circ G(\Sigma Z_\mu t^\mu) = G^{-1}(\Sigma G_\mu t^\mu) = G^{-1}(\exp(\sum_{i=1}^{\infty} X_i t^i)) =$$

$$= \exp(\sum_{i=1}^{\infty} G^{-1}(X_i) t^i).$$

Put $G^{-1}(X_i) = Y_i$. Because $X_i \in P(Z)$ and G^{-1} is a curve, $Y_i \in P(Z)$. Because G_μ is isobaric of weight μ, one concludes that Y_i is isobaric of weight i and that

$$(3.12)\quad Y_i = Z_i + h_i(Z_{i-1},\ldots,Z_1).$$

The Y_i are obviously unique. We now have proven the first part of:

3.5.2. Theorem. (Campbell-Hausdorff). Let Z be the UNG over k, $\chi(k) = 0$. Then:

a There exists a unique family $\{Y_i\}_{i\geq 1} \subset P(Z) \subset Z$. $Y_i = Z_i + h_i(Z_{i-1},\ldots,Z_1)$, Y_i is isobaric of weight i. $Z = k\langle Y_i\rangle_{i\geq 1}$ and

$$\Sigma Z_\mu t^\mu = \exp(\sum_{i=1}^{\infty} Y_i t^i).$$

b Let $G \in GCoalg_k$ and let $\phi = \Sigma \phi_\mu t^\mu$ be a curve in G. Then there exists a unique family $\{\xi_i\}_{i\geq 1} \subset P(G)$ such that

$$\Sigma \phi_\mu t^\mu = \exp(\sum_{i=1}^{\infty} \xi_i t^i).$$

c There exists a unique family $\{z_i\}_{i\geq 1}$ of polynomial functions in non-commuting variables U_i, V_j, $z_i = z_i(U_i,\ldots,U_1,V_i,\ldots,V_1)$, such that for any $G \in GCoalg_k$ and any two curves $\exp(\sum_{i=1}^{\infty} \xi_i t^i)$ and $\exp(\sum_{i=1}^{\infty} \eta_i t^i)$ in G the following formula holds:

$$(3.12a)\quad \exp(\sum_{i=1}^{\infty} \xi_i t^i) \exp(\sum_{i=1}^{\infty} \eta_i t^i) = \exp(\sum_{i=1}^{\infty} z_i(\xi_i,\ldots,\xi_1,\eta_i,\ldots,\eta_1) t^i).$$

Proof. a has already been established.

b $\phi : Z \to G$ induces a continuous homomorphism of groups $H(\phi) : H(Z) \to H(G)$

such that $\phi = H(\phi)(\Sigma Z_\mu t^\mu) = H(\phi)(\exp(\sum_{i=1}^{\infty} Y_i t^i)) = \exp(\sum_{i=1}^{\infty} \phi(Y_i)t^i)$. Put $\xi_i = \phi(Y_i)$.

Considering $\exp(\sum_{i=1}^{\infty} \xi_i t^i) \in G[[t]]$ as a formal powerseries in t, (3.12) gives that $\xi_i = \phi(Y_i) = \phi_i + h_i(\phi_{i-1},\dots,\phi_1)$ for all $i \geq 0$. The unicity of the family $\{\xi_i\}_{i\geq 1}$ follows easily from this: if $\phi = \exp(\sum_{i=1}^{\infty} \eta_i t^i)$, $\eta_i \in P(G)$, then the η_i must satisfy the same relations $\eta_i = \phi_i + h_i(\phi_{i-1},\dots,\phi_1)$. By recurrency $\eta_i = \xi_i$ for all i.

c Let $W = k\langle U_i, V_i\rangle_{i\geq 1}$ be in $GCoalg_k$, $\{U_i,V_i\}_{i\geq 1} \in P(W)$. The product-curve $\phi_1\phi_2$ in W of $\phi_1 = \exp(\sum_{i=1}^{\infty} U_i t^i)$ and $\phi_2 = \exp(\sum_{i=1}^{\infty} V_i t^i)$ is again a curve in W and by b of this this theorem, there exists a unique family $z_i \in P(W)$ such that $\phi_1\phi_2 = \exp(\sum_{i=1}^{\infty} z_i t^i)$.

Notice that if one attaches to U_i and V_i the weight i, z_i is isobaric of weight i. Now the families $\{\xi_i\}_{i\geq 1}$ and $\{\eta_i\}_{i\geq 1}$ in P(G) define a morphism $\psi : W \to G$ in $GCoalg_k$, $\psi(U_i) = \xi_i$, $\psi(V_i) = \eta_i$. The induced group-homomorphism $H(\psi) : H(W) \to H(G)$ gives $H(\psi)(\phi_1).H(\psi)(\phi_2) = H(\psi)(\phi_1\phi_2)$ and this is infact (3.12a). The unicity of the z_i is obvious.

3.5.3. The whole story repeats itself over a field k, $\chi(k) = p > 0$.

Let $Z = k\langle X_{ij}\rangle_{(i,j)\in S}$ be the UNG over k (3.3.2.cor 2). In (3.4.2.) we have defined a non associative operation $\curlywedge$ on L(Z). In view of this we define $\curlywedge_{i=1}^{n} \xi_i$ inductively by $\curlywedge_{i=1}^{n} \xi_i = (\curlywedge_{i=1}^{n-1} \xi_i) \curlywedge \xi_n$ and $\curlywedge_{n=1}^{1} \xi_i = \xi_1$.

Fix $n \geq 0$ and consider $S_n \underset{\text{Def}}{=} \curlywedge_{j=1}^{n} ((X_{ij})_{i\geq 0})$, where it must be understood that $X_{ij} = 0$ if $(j,p) = p$. S_n being an E-pure set in Z, we write $S_n = (S_{i,n})_{i\geq 0}$ and the E-pure curve, defined by S_n will be denoted $F_n = F_{n,\mu}t^\mu$.

Assign to each X_{ij} the weight jp^i (3.3.1. th.a), then d is compatible with the weight, i.e. dX_{ij} is isobaric of total weight jp^i, hence we can follow the construction of (3.5.1). Put again $F_{n,\mu} = \sum_{\rho=0}^{\infty} F_{n,\mu,\rho}$ as a unique

(finite) sum of isobaric parts and consider

$$G^{(n)} = \sum_{\rho=0}^{\infty} \Big(\sum_{\mu=0}^{\infty} F_{n,\mu,\rho} \Big) t^{\rho} = \sum_{\rho=0} G_{\rho}^{(n)} t^{\rho}.$$

This is well defined because $F_{n,\mu,\rho} = 0$ if $\mu > \rho$. We thus may conclude as in (3.5.1): $G^{(n)}$ is a curve in Z.

Lemma. $G^{(n)} \equiv G^{(n+1)} \pmod{t^{n+1}}$.

Proof. This is trivial if $(n+1,p) = p$ for then $S_{n+1} = S_n$. Thus let $(n+1,p) = 1$. Then $S_{n+1} = S_n \times (X_{i,n+1})_{i\geq 0}$ and by (3.4) we have

$$(3.13) \qquad S_{i,n+1} = S_{i,n} + X_{i,n+1} + g_i(S_{i-1,n},\ldots,S_{0,n},X_{i-1,n+1},\ldots,X_{0,n+1}).$$

Because $g_i(S_{i-1,n},\ldots,S_{0,n},0,\ldots,0) = 0$ (3.4.2a), each term in g_i contains at least a factor $X_{j,n+1}$ for some j, hence

$$(3.14) \qquad S_{i,n+1} = S_{i,n} + \text{terms having at least weight } n+1.$$

From this the lemma will be clear.

If $\chi(k) = 0$ we may consider the exponential series as a function $\exp : \underline{r} \to 1+\underline{r} \subset Z[[t]]$, where $\underline{r}$ is the two-sided ideal in $Z[[t]]$ generated by t. If $\chi(k) = p > 0$, let CS be the set of sequences $(\xi_i)_{i\geq 0} \subset \underline{r}$ in $Z[[t]]$ converging to zero in the (t)-adic topology. Then the canonical E-pure curve defines a function $E : CS \to 1+\underline{r}$, $E((\xi_i)_{i\geq 0}) = E(\xi_0,\xi_1,\ldots) = \sum_{i=0}^{\infty} E_{\mu}(\xi_0,\ldots,\xi_{\mu})$. In order to show that this sum converges in the (t)-adic topology, it suffices to show: if $N > 0$ is given, there exists only a finite number of monomials $X_0^{\alpha_0}\ldots X_r^{\alpha_r}$, $\alpha_i \geq 0$, r arbitrary, such that $\xi_0^{\alpha_0}\ldots\xi_r^{\alpha_r} \not\equiv 0 \pmod{t^N}$. Now: if r is large enough, $\xi_r \equiv 0 \pmod{t^N}$, hence r must run over a finite interval.

Further, if ξ_i is given then there exists β_i such that $\xi_i^{\beta_i} \equiv 0 \pmod{t^N}$, because $\xi_i \in \underline{r}$. Thus $E : CS \to 1+\underline{r}$ is well defined.

By (3.13) consider S_{ij} as a polynomialfunction in the X_{ab} with $bp^a \leq jp^i$ and let T_{ij} be the element of $\underline{r} \subset Z[[t]]$ obtained from S_{ij} by substituting $X_{ab}t^{bp^a}$ for X_{ab}. Then:

$$\lim_{j\to\infty} T_{ij} = g_i(X_{ab},t) = T_i \tag{3.15}$$

exists and $(T_i)_{i\geq 0} \in CS$ as follows from (3.13).

It follows from the construction that

$$G^{(n)} = E(T_{0n},T_{1n},\ldots)$$

$$G = \Sigma G_\mu t^\mu = \lim_{n\to\infty} G^{(n)} = E(T_0,T_1,\ldots). \tag{3.16}$$

Here G_μ is isobaric of weight μ (by construction) and because each X_{ij} occurs, we have

$$G_{jp^i} = X_{ij} + f_{ij}(X_{ab}) \tag{3.17}$$

where f_{ij} is a polynomial in the X_{ab} satisfying $bp^a < jp^i$, hence the curve G defines an automorphism $G : Z \to Z$ in $GCoalg_k$.
Extend G and G^{-1} to $Z[[t]]$ in $NAlg_k$ by defining $G(t) = G^{-1}(t) = t$. It follows:

$$\begin{aligned} \Sigma Z_\mu t^\mu = G^{-1} \circ G(\Sigma Z_\mu t^\mu) = G^{-1}(\Sigma G_\mu t^\mu) &= G^{-1}(E(T_0,T_1,\ldots)) \quad (3.16)\\ &= E(G^{-1}(T_0),\ G^{-1}(T_1),\ldots)\\ &= E(P_0,P_1,\ldots) \quad , \text{ putting } G^{-1}(T_i) = P_i,\ i \geq 0. \end{aligned} \tag{3.18}$$

Here $G^{-1}(T_i) = g_i(G^{-1}(X_{ab}),t)$. Put $G^{-1}(X_{ab}) = Y_{ab}$ then we have by (3.17):

$$Z_{jp^i} = Y_{ij} + f_{ij}(Y_{ab}) \quad , \quad bp^a < jp^i. \tag{3.19}$$

Because G is an isobaric curve, Y_{ab} is isobaric of weight bp^a for all (a,b) and we can solve Y_{ij} uniquely in terms of Z_{bp^a}, giving

(3.20) $$Y_{ij} = Z_{jp^i} + h_{ij}(Z_{bp^a}).$$

Notice that in view of $Y_{ij} = G^{-1}(X_{ij})$, the Y_{ij} are E-pure. The set $(Y_{ij})_{i\geq 0}$ is E-pure for every j.

We thus have proven the first part of

3.5.4. Theorem. (Campbell-Hausdorff-Dieudonné). Let Z be the UNG over k, $\chi(k) = p > 0$. Then:

a There exists a family of free generators $\{Y_{ij} \mid (i,j) \in S\}$ of Z over k, $S = \{(i,j) \in \mathbb{Z} \times \mathbb{Z} \mid i \geq 0,\ j \geq 1,\ (j,p) = 1\}$, uniquely determined by the following conditions:

a1 : The set $(Y_{ij})_{i\geq 0}$ is E-pure for every j, $Y_{ij} = Z_{jp^i} + h_{ij}(Z_{bp^a})$.

a2 : $P_m = g_m(Y_{ab},t)$, $m \geq 0$ (3.15).

a3 : $\Sigma Z_\mu t^\mu = E(P_0,P_1,\ldots)$.

b Let $G \in GCoalg_k$ and let $\Sigma\phi_\mu t^\mu$ be a curve in G. Then there exists a family $\{\xi_{ij}\}_{(i,j)\in S} \subset G$, uniquely determined by:

b1 : $(\xi_{ij})_{i\geq 0}$ is an E-pure set for every j.

b2 : $\xi_m = g_m(\xi_{ab},t)$.

b3 : $\phi = E(\xi_0,\xi_1,\ldots)$.

c There exists a family $\{\phi_{ij}\}_{(i,j)\in S}$ of polynomial functions in non commuting weighted indeterminates U_{ij}, V_{ij}, having weight jp^i, uniquely determined by:

c1 : ϕ_{ij} is isobaric of weight jp^i.

c2 : Let G be in $GCoalg_k$ and let $\{\xi_{ij}\}_{(i,j)\in S}$ and $\{\eta_{ij}\}_{(i,j)\in S}$ be families in G, satisfying b1, b2 and b3. Put $\xi_m = g_m(\xi_{ab},t)$, $\eta_m = g_m(\eta_{ab},t)$, $\zeta_{ij} = \phi_{ij}(\xi_{ab},\eta_{cd})$ and $\zeta_m = g_m(\zeta_{ij},t)$. Then

(3.21) $$E(\xi_0,\xi_1,\ldots)\,E(\eta_0,\eta_1,\ldots) = E(\zeta_0,\zeta_1,\ldots).$$

Proof. a has already been established.

b Put $\xi_{ij} = \phi(Y_{ij})$, then the existence of the family $\{\xi_{ij}\}_{(i,j)\in S'}$ satisfying b2 and b3 is obvious. As for the unicity, remark that $E(\xi_0,\xi_1,\ldots) = \Sigma\phi_\mu t^\mu$, where ϕ_{jp^i} has the form $\phi_{jp^i} = \xi_{ij} + f_{ij}(\xi_{ab})$. If $\{\eta_{ij}\}_{(i,j)\in S}$ is a family in G, satisfying b1, b2 and b3, then b2 implies that the η_{ij} satisfy the same relations $\phi_{jp^i} = \eta_{ij} + f_{ij}(\eta_{ab})$. By recurrency $\xi_{ij} = \eta_{ij}$ for all i and j.

c Let $W = k\langle U_{ij},V_{ij}\rangle_{(i,j)\in S} \in \mathrm{GCoalg}_k$ such that $(U_{ij})_{i\geq 0}$ and $(V_{ij})_{i\geq 0}$ are E-pure sets for every j. Put $U_m = g_m(U_{ab},t)$ and $V_m = g_m(V_{ab},t)$, then $E(U_0,U_1,\ldots)\,E(V_0,V_1,\ldots) = E(W_0,W_1,\ldots)$ and by b of this theorem we have $W_m = g_m(W_{ij},t)$ for a unique family $\{W_{ij}\}_{(i,j)\in S}$ in W. Put $W_{ij} = \phi_{ij}(U_{ab},V_{cd})$. (3.21) is clear from functoriality. (3.17) and the fact that a product of isobaric curves is again an isobaric curve, applied to $E(U_0,U_1,\ldots)\,E(V_0,V_1,\ldots)$, show that the ϕ_{ij} are isobaric. c2 shows that the ϕ_{ij} are solutions of a universal problem, hence the ϕ_{ij} are unique.

3.5.5. Remark. J.A. Dieudonné was the first who obtained a Campbell-Hausdorff-theorem over the prime fields $\mathbb{F}_p$, $p > 0$. See [5, formula (68)] and the review of P. Cartier, MR 20-930.
We included the theorem here, because it is an essential theorem in the theory of curves and because the proof is different from the proof, given by J.A. Dieudonné. Moreover, assertion b3, namely that each curve ϕ can be written as $\phi = E(\xi_0,\xi_1,\ldots)$, is a generalisation of the formula, given by J.A. Dieudonné. The observation that the groupstructure of $\mathrm{Al}_k(G,k[[t]])$, $G \in \mathrm{ICAl}_k$ is essentially given by the Campbell-Hausdorff-Dieudonné formula seems to be new. From this again it is obvious that the formal cogroups $G \in \mathrm{ICAl}_k$ cannot in general be recovered from

Lie $G = Al_k(G,k[t]/(t^2)) = H_1(G^*)$ if $\chi(k) = p > 0$. The classification of commutative formal groups in the sense of Dieudonné as given by P. Cartier in [8] and [9], making use of the group of curves, suggests that in the general case, it might be possible to recover $G \in ICAl_k$ from the group $Al_k(G,k[[t]])$.

In Ch. IV we shall show that this is true in the following sense: G is determined up to isomorphism by the E-pure semiderivations in G . We have proven it there for a certain class of formal cogroups. Finally notice that there can be made Campbell-Hausdorff-Dieudonné statements for finite curves.

CHAPTER IV

Comments and open questions

4§1 Application to a structure theory of formal cogroups.

4.1.1. Let k be an arbitrary field, $\chi(k) = p > 0$ and let $\bar{k}$ be a perfect closure of k. Denote $C(n)^*$ the full subcategory of $B \in ICAl_k$, such that $\bar{B} = B \otimes_k \bar{k}$ has height $\leq n+1$. There is a canonical inclusion functor $C(n)^* \hookrightarrow C(n+1)^*$. Moreover, by [PGB 4.4.2.] each $B \in ICAl_k$ is projective limit in $ICAl_k$ of the cogroups $B/I^{(p^n)}$, where $I = \mathrm{Ker}\,\{\varepsilon : B \to k\}$ and $I^{(p^n)}$ is the closed ideal in B, generated by $\{x^{p^n} \mid x \in I\}$. Because $B/I^{(p^{n+1})} \in C(n)^*$, it follows that a structure theory of the categories $C(n)^*$, $n \geq 0$ is a first step in a structure theory for $ICAl_k$. By Cartier-duality we may as well consider the full subcategory C(n) of $GCoalg_k$, consisting of $G \in GCoalg_k$ such that $G^* \in C(n)^*$.

4.1.2. Definition. Let $G \in C(n)$. An ordered p-base $\{\xi_{ij} \mid j \in T, 0 \leq i \leq N(j) \leq n\}$ for G, where T is an ordered set, will be called an E-base for G if for every $j \in T$ the set $(\xi_{ij})_{0 \leq i \leq N(j)}$ is E-pure.

From the proof of proposition (3.3.4) it follows that every $G \in C(n)$ admits an E-base. (3.3.4) gives equally that for every $G \in C(n)$ there exists a surjective morphism $\phi : U(n)^{(T)} \to G$ in $GCoalg_k$.
Notice that $U(n) \in C(n)$. As usual we write $U(n) = k\langle X_0, \ldots, X_n \rangle$.

4.1.3. Definition. Let $r \geq 0$ be an integer and define the covariant functor $S_r : GCoalg_k \to Sets$ by

$$S_r(G) = \{\text{E-pure semiderivations of height} \leq r \text{ in } G\}.$$

We recall that $L_r : GCoalg_k \to Sets$ is defined by $L_r(G) = GCoalg_k(U(r), G)$.

4.1.4. Lemma. The functormorphism $\psi : L_r \to S_r$, defined for $G \in GCoalg_k$ by

$\psi(G)(f) = f(X_r)$ is a functor isomorphism.

Proof. Let $u \in G^*$ and let $f^* : G^* \to U(r)^*$ be the transposed morphism. Then $\langle f(V^i X_r), u\rangle = \langle V^i X_r, f^*(u)\rangle = \langle X_r, f^*(u^{p^i})\rangle^{1/p^i} = \langle V^i f(X_r), u\rangle$. Hence $f(V^i X_r) = V^i f(X_r)$ and thus f is determined by the value $f(X_r)$. If $\xi \in S_r(G)$, $V^i\xi$ is defined for every $i \geq 0$ and the relation $(\phi(G)(\xi))(X_r) = \xi$ defines a functor morphism, inverse to ψ.

It follows from the lemma that the structure on $L_r(G)$, defined in (3.4.3) can be carried over to $S_r(G)$. Explicitly: For $x,y \in S_r(G)$ we have

$$x \ast y = x + y + g_r(Vx,\ldots,V^r x,Vy,\ldots,V^r y) \qquad (3.4)$$

(4.1)
$$cx = -x + h_r(Vx,\ldots,V^r x) \qquad (3.5)$$

$$Fx = x^p + f_r(Vx,\ldots,V^r x) \qquad (3.6)$$

$$(x,y) = xy - yx + c_r(x,\ldots,V^r x,y,\ldots,V^r y) \qquad (3.7)$$

$$\lambda \ast x = \lambda^{p^r} x. \quad (\lambda \in k) \qquad (3.8)$$

These operations are functorial in $G \in GCoalg_k$. We shall from now on only write $\lambda^{p^r} x$. The notation $\lambda \ast x$ will not be used.

4.1.5. Lemma. Let $G \in C(n)$. The sequence of morphisms in $GCoalg_k$, $\ldots \to U(r) \xrightarrow{f_r} U(r-1) \xrightarrow{f_{r-1}} \ldots \to U(0)$, defined by $f_{r-i}(X_{r-i}) = X_{r-i-1}$, $i \geq 0$, induces an sequence of inclusions $S_0(G) \hookrightarrow \ldots \hookrightarrow S_{r-1}(G) \hookrightarrow S_r(G) \hookrightarrow \ldots$ Then: $\varinjlim_r S_r(G) = S_n(G) = \{\text{Set of E-pure semiderivations in } G\}$.

Proof. Let $\xi \in S_{n+m}(G)$, then ξ defines an E-pure set $(\eta_0,\ldots,\eta_{n+m})$, $\eta_{n+m} = \xi$. From the relation $0 = \langle \eta_{n+m}, x^{p^{n+1}}\rangle = \langle \eta_{m-1}, x\rangle^{p^{n+1}}$, $x \in G^*$ it follows that $\eta_{m-1} = 0$, hence $\eta_\mu = 0$ for $0 \leq \mu \leq m-1$. By lemma (3.4.2d), the set $(\eta_m,\ldots,\eta_{m+n})$ is E-pure, hence $\xi = \eta_{m+n}$ has height $\leq n$ and belongs to $S_n(G)$.

Conjecture: If $\varinjlim_r S_r(G) = S_n(G)$ and $G^* \in ICAl_k$, then $G \in C(n)$.

4.1.6. Proposition. Let $G \in C(n)$. Define for $x_0,\ldots,x_N \in S_n(G)$, $\overset{N}{\underset{i=0}{\Sigma^*}} x_i$ inductively by $\overset{N}{\underset{i=0}{\Sigma^*}} x_i = (\overset{N}{\underset{i=1}{\Sigma^*}} x_i) * x_0$ and $\overset{N}{\underset{i=N}{\Sigma^*}} x_i = x_N$.

Let $\{\xi_{ij} \mid j \in T,\ 0 \leq i \leq N(j) \leq n\}$ be an E-base for G (4.1.2) and let $x \in S_n(G)$. Then there exist unique $\lambda_{ij} \in k$, almost every λ_{ij} is zero, such that

$$x = \overset{n}{\underset{i=0}{\Sigma^*}} \left(\Sigma^*_j \lambda_{ij}^{p^i} \xi_{ij}\right)$$

and such that $V^{s+1}x = 0$, $\lambda_{ij} \neq 0$ implies $i \leq s$.

Proof. We proceed by recurrency with respect to the subsets $S_r(G)$, $0 \leq r \leq n$. Let $x \in S_0(G) = P(G)$. It then is clear that

$$x = \Sigma_j \lambda_{0j} \xi_{0j} = \Sigma^*_j \lambda_{0j} \xi_{0j}.$$

(We tacitly assume that Σ^*_j denotes a finite ordered sum). Now assume that, if $r \geq 0$ and $x \in S_r(G)$, there exist unique $\mu_{ij} \in k$, such that

$$x = \overset{r}{\underset{i=0}{\Sigma^*}} \left(\Sigma^*_j \mu_{ij}^{p^i} \xi_{ij}\right) \tag{4.2}$$

and such that $V^{s+1}x = 0$, $\mu_{ij} \neq 0$ implies $i \leq s$.

Let $y \in S_{r+1}(G)$, then $Vy = x \in S_r(G)$, thus assume that $Vy = x$ has the form (4.2). We claim: if $\mu_{ij} \neq 0$ in (4.2) and $x = Vy$, then $i < N(j)$, hence $\xi_{i+1,j}$ is an element of the E-base, thus

$$z = \overset{r}{\underset{i=0}{\Sigma^*}} \left(\Sigma^*_j \mu_{ij}^{p^{i+1}} \xi_{i+1,j}\right) \in S_{r+1}(G). \tag{4.3}$$

Indeed: observe that for $x,y \in S_n(G)$, $x * y = x+y + a(x,y)$ where $a(x,y) \in \operatorname{Im} V$ (4.1), because g_n is a universal polynomial, rational over $\mathbb{F}_p$. More generally it follows that

$$Vy = x = \overset{r}{\underset{i=0}{\Sigma}} \Sigma_j \mu_{ij}^{p^i} \xi_{ij} + s(x), \qquad s(x) \in \operatorname{Im} V. \tag{4.4}$$

Thus $x-s(x) \in \operatorname{Im} V$ and $x-s(x)$ is a linear combination of elements of the

E-base. Because the E-base together with $0 \in G$ is closed under the action of V, given by $V\xi_{ij} = \xi_{i-1,j}$, we conclude that $\sum_{i=0}^{r} \sum_{j} \mu_{ij}^{p^i} \xi_{ij} \in \operatorname{Im} V$ iff $\mu_{ij} \neq 0$ implies $i < N(j)$. Using the relation $V(x \star y) = Vx \star Vy$, (4.3) gives $Vz = Vy = x$, so $V(z-y) = 0$, implying $z-y \in S_0(G)$.

It follows:

$$y = z + \sum_j \nu_{0j} \xi_{0j} = z + \sum_j^{\star} \nu_{0j} \xi_{0j} = z \star \sum_j^{\star} \nu_{0j} \xi_{0j}, \tag{4.5}$$

and (4.3) substituted in (4.5) proves the induction step. The proposition now is evident.

4.1.7. Let $G \in C(n)$ and let $\{\xi_{ij} \mid j \in T,\ 0 \leq i \leq N(j) \leq n\}$ be an E-base for G. This E-base determines a surjective morphism $\psi : \coprod_j U(N(j)) \to G$ in $GCoalg_k$ as follows: Let $\coprod_j U(N(j)) = k\langle X_{ij} \rangle_{j \in T,\ 0 \leq i \leq N(j)}$, then $\psi(X_{ij}) = \xi_{ij}$. From proposition (4.1.6) it follows that every E-pure element in G can be lifted to an E-pure element in $\coprod_j U(N(j))$.
We may use this in order to show that $\ker \psi$ is generated by E-pure elements. Indeed: the E-base defines an ordered p-base for the k-vectorspace G, hence the structure of G as an object in $GCoalg_k$ is determined, if one knows how to express the ξ_{ij}^p and the commutators $\xi_{ij}\xi_{ab} - \xi_{ab}\xi_{ij}$ in terms of this ordered p-base. (the diagonal of G is determined by the E-purity of the ξ_{ij}). Now by (4.1) we have:

$$\begin{aligned} F\,\xi_{ij} &= \xi_{ij}^p + f_i(\xi_{i-1,j}, \ldots, \xi_{0j}) \\ &= \sum_{a=0}^{\star} (\sum_b{}^{\star} \lambda_{ijab}^{p^a} \xi_{ab}) \qquad (4.1.6) \end{aligned} \tag{4.6}$$

and $\lambda_{ijab} \neq 0$ implies $a \leq i$ (4.6) can be lifted in order to give

$$F\,X_{ij} \equiv \sum_{a=0}^{\star} (\sum_b{}^{\star} \lambda_{ijab}^{p^a} X_{ab}) \pmod{\operatorname{Ker} \psi}. \tag{4.7}$$

First observe that (4.7) gives a relation for X_{ij}^p, because the right hand side of (4.7) does not contain any monomial involving X_{ij}^p. On the otherhand

however, if $x_0 \equiv y_0 \pmod{\mathrm{Ker}\ \psi}$ and x_0, y_0 are E-pure, then $x_0 - y_0$ in general is not an E-pure semiderivation, but we can modify this in order to find an E-pure semiderivation as follows: define x_i and y_i inductively by $x_i = (cx_{i-1}) \star x_{i-1}$ and $y_i = (cx_{i-1}) \star y_{i-1}$. Now $V^r x_i = 0$ implies $V^{r-1} x_{i+1} = 0$, thus if i is large enough, we arrive at a congruence $0 = x_i \equiv y_i \pmod{\mathrm{Ker}\ \psi}$, hence y_i is an E-pure semiderivation in Ker ψ. Applying this procedure to (4.7) we find an E-pure semiderivation in Ker ψ that gives a relation for X_{ij}^p. For the commutators $\xi_{ij}\,\xi_{ab} - \xi_{ab}\,\xi_{ij}$ we can proceed in the same way.

Observe that if $x \in$ Ker ψ and if x is an E-pure semiderivation, then $Vx \in$ Ker ψ. Indeed: if ψ^* is the transposed morphism and $u \in G^*$ then $\langle \psi(Vx), u \rangle = \langle Vx, \psi^*(u) \rangle = \langle x, \psi^*(u^p) \rangle^{1/p} = \langle \psi(x), u^p \rangle^{1/p} = 0$. On the other hand, if H is a direct sum of copies of U(i), $0 \leq i \leq n$ in GCoalg_k, and if $\mathcal{A}$ is a twosided ideal in H, generated by E-pure semiderivations x satisfying the condition that Vx again belongs to $\mathcal{A}$, then $H/\mathcal{A}$ has a natural induced structure of groupcoalgebra, because $dx \in \mathcal{A} \otimes H + H \otimes \mathcal{A}$, $\varepsilon(x) = 0$ and cx can be expressed in the $V^i x$, $i \geq 0$.

4.1.8. At this time the author cannot give stronger assertions about the structure of objects of C(n). If n = 0, the known structure of infinitesimal cogroups of height ≤ 1 can easily be recovered from (4.1.7): $S_0(G)$ has a natural structure of p-Liealgebra over k ((3.4.4). The case p = 2 is only a slight modification). In order to arrive at a good structure theory along the pattern of E-pure semiderivations, one should be able to give intrinsic definitions for the operations (4.1). But even if n = 0, the second formula of Jacobson, [PGA 5.1], giving $F(x \star y)$ in terms of F, $\star$ and (,), shows that the technical difficulties will be considerable. One then has still the problem that the E_μ-polynomials are not unique.

4.1.9. In the commutative case, the connection between the known struc-

ture theory of affine commutative unipotent groupschemes over a perfect groundfield, as given in [SHS, th. 8.4] and the notion of E-pure semiderivation is obvious: with the notations of loc.cit. let Spec H be unipotent, $H \in Ab_k$, then:

$$\mathcal{D}(\text{Spec } H) = \varinjlim_{n} Gr(\text{Spec } H, W_n) \xrightarrow[(3.1.8)]{\sim} \varinjlim_{n} Ab_k(A(n),H) = \varinjlim_{n} S_n(H),$$

hence:

$$\mathcal{D}(\text{Spec } H) = \text{Set of all pure semiderivations in } H.$$

In particular, restricting $\mathcal{D}$ o Spec to the full subcategory AC(n) of $H \in Ab_k \subset GCoalg_k$, such that $H \in C(n)$, one has by (4.1.5)

$$\mathcal{D}(\text{Spec } H) \xrightarrow{\sim} \varinjlim_{r} S_r(H) = S_n(H)$$

and S_n defines an equivalence between AC(n) and the category of modules over the endomorphism ring $D(n) = S_n(A(n))$. This implies in particular that A(n) is a projective generator of the category AC(n).

If k is not perfect, (4.1.7) gives at least an idea how the objects of AC(n) look like and if $H \in AC(n)$, then it is possible to recover H from $S_n(H)$, but as P. Gabriel kindly did observe to the author, S_n is not an exact functor if k is not perfect and if $n > 0$. We give an easy example for this: Let $A(1) \xrightarrow{f} A(0)$ be the epimorphism in AC(1), $f(X_1) = X_0$, $f(X_0) = 0$. From (4.1.6) it follows that $x \in S_1(A(1))$ can uniquely be put in the form $x = \sum_j{}^{*} \lambda_{ij}^{p^j} X_1^{p^j} * \sum_j{}^{\wedge} \lambda_{0j} X_{0j}^{p^j}$, because the set $\{X_i^{p^j} \mid 0 \leq i \leq 1,\ j \geq 0\}$ is an E-base for A(1). Now $S_1(f)(x) = \sum_j \lambda_{ij}^{p^j} X_0^{p^j}$ and it is clear that if $\lambda \in k$, $\lambda \notin k^p$, λX_0 cannot be lifted under f to an E-pure semiderivation in A(1).

A(n) however is still a generator in the category AC(n): Let $g : B \to C$ be a monomorphism in AC(n), i.e. g is injective, and suppose that $\bar{g} = S_n(g) : S_n(B) \to S_n(C)$ is a bijection. By (4.1.6), the elements of $S_n(B)$

and $S_n(C)$ can be described by E-bases for B and C. Bijectivity of $\bar{g}$ then means that every element in an E-base for C can be expressed in terms of an E-base for B, i.e. $g(B) = C$. This expresses that A(n) is a generator. By the Gabriel-Popescu theorem[10,6.25]we then have that the category AC(n) is equivalent with a certain quotient category of the category of $S_n(A(n))$-modules.

4§2 Open questions.

4.2.1. The UNG is already defined over $\mathbb{Z}$, Put $UNG_{\mathbb{Z}} = Z'$. The decompositiontheorem shows that $k \otimes_{\mathbb{Z}} Z$ decomposes over every prime field k. The construction of Dieudonné for the hyper exponential series suggests that $\mathbb{Z}_p \otimes_{\mathbb{Z}} Z'_{comm}$ decomposes, where Z'_{comm} is the largest commutative quotient of Z' and $\mathbb{Z}_p$ is the ring of p-adic integers. Is it true that $\mathbb{Z}_p \otimes_{\mathbb{Z}} Z'$ decomposes over $\mathbb{Z}_p$? It might happen that in that case there is a canonical choice for the E_μ-polynomials. Z' seems to be indecomposable.

4.2.2. It is conceivable that the theory of E-pure semidcrivations can give information concerning the (local) structure of algebraic groups, defined over fields of positive characteristic.
We only give an easy example:

Let k be a field, $\chi(k) = 2$ and G the groupfunctor $Alg_k \to$ Groups, defined by

$$G(B) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & a^2 & b \\ 0 & 0 & 1 \end{pmatrix} , \text{ a unit in B, } b \in B \right\}. \quad [11,\ 10.\bar{v}].$$

The groupstructure is defined by ordinary product of matrices.
Then Lie $G = \mathrm{Ker}\ \{G(k[t]/(t^2)) \to G(k)\}$ can be represented by the set of matrices $\left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix} \mid a,b \in k \right\}$ and is abelian, while G is not a commu-

tative groupfunctor. As Chevalley remarked, G(k) is not contained in the algebra over k, generated by Lie G.

Now Ker $\{G(k[t]/(t^3)) \to G(k)\}$ can be represented by the curves

$$(4.8)\qquad \{I + \begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & 0 & \beta_1 \\ 0 & 0 & 0 \end{pmatrix} t + \begin{pmatrix} \alpha_2 & 0 & 0 \\ 0 & \alpha_1^2 & \beta_2 \\ 0 & 0 & 0 \end{pmatrix} t^2 \mid \alpha_1,\alpha_2,\beta_1,\beta_2 \in k\}.$$

As follows from the theory of E-pure semiderivations, the coefficient of t^2 is unique up to a derivation, in particular $\begin{pmatrix} 0 & 0 & 0 \\ 0 & \alpha_1^2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ is an E-pure semiderivation of G, and G(k) is contained in the not abelian k-algebra generated by the E-pure semiderivations. One verifies easily that there are no other E-pure semiderivations of strict greater height.

It should be noted, that putting $t = 1$ in (4.8) and $\alpha_2 = \beta_2 = 0$, $\alpha_1 \neq 1$, the group generated by $I + \begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & 0 & \beta_1 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & \alpha_1^2 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1+\alpha_1 & 0 & 0 \\ 0 & (1+\alpha_1)^2 & \beta_1 \\ 0 & 0 & 1 \end{pmatrix}$ is isomorphic with G(k). The author has no general results in this direction

4.2.3. The use of semiderivations in the theory of inseparable field extensions is well known by the work of Dieudonné, Jacobson, Sweedler a.o. The question could arise if the notion of E-purity is able to give more detailed information.

4.2.4. The notion of E-purity cuts short the classification of (abelian) formal groups of dimension 1 over a separably closed field as given in [2. §8]. Indeed: Let G be such a formal group with coordinate ring $k[[X]]$. Let $\psi = \Sigma E_\mu(\xi_0,\ldots,\xi_\mu)t^\mu$ be the E-pure curve belonging to the canonical curve $k[[X]] \to k[[t]]$, $X \longmapsto t$. If G^* is the Cartierdual of the formal cogroup $k[[X]]$, then the E-pure set $(\xi_i)_{i\geq 0}$ is a p-base for G^*, and thus the structure of G is completely known if one knows the relations for ξ_i^p, $i \geq 0$. But these are given by the E-pure curve ψ^p, defined by the E-pure set

$(0,\xi_0^p,\xi_1^p,\ldots)$. Now the arguments of Dieudonné apply: If $\xi_i^p = 0$, $i \geq 0$ then $G \simeq A/(X_i^p)_{i\geq 0}$ and G is the additive formal cogroup.

If $\xi_0^p \neq 0$, then, ξ_0^p being primitive, one can carry out a base transformation such that G^* has a p-base of E-pure elements, $(\eta_i)_{i\geq 0}$ satisfying $\eta_i^p = \eta_i$, $G^* \simeq A/(X_i^p - X_i)_{i\geq 0}$ and G is the multiplicative formal group.

Finally, let j be the least integer such that $\xi_j^p \neq 0$, then ξ_j^p is primitive. After a suitable transformation, as given in Dieudonné, one finds $G^* \simeq A/(X_i^p - X_{i-j})_{i\geq 0}$. Thus in all cases we can put $G^* \simeq A/(X_i^p - X_{i-j})_{i\geq 0}$, $0 \leq j \leq \infty$. (Put $X_\nu = 0$ if $\nu < 0$), and there are no problems about the existence of formal groups having the hyperalgebra $A/(X_i^p - X_{i-j})_{i\geq 0}$.

BIBLIOGRAPHY

PGA P. Gabriel, SGAD '63-'64, Exp VIIA.

PGB P. Gabriel, SGAD '63-'64, Exp VIIB.

PCL P. Cartier, Séminaire Sophus Lie, 2^{e} année.

SHS Séminaire Heidelberg-Strasbourg. Exp 11.

1 J. Dieudonné, Groupes de Lie et hyperalgèbres... I.
Comm.Math.Helv. 28(1954), 87-117.

2 J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic p > 0. II
Am.J. of Math. 77(1955), 218-244.

3 J. Dieudonné, Groupes de Lie et hyperalgèbres... III.
Math.Zeitschr. 63(1955), 53-75.

4 J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic p > 0. IV.
Am.J. of Math. 77(1955), 429-452.

5 J. Dieudonné, Groupes de Lie et hyperalgébres... V.
Bull.Soc.Math.France. 84(1956), 207-239.

6 J. Dieudonné, Witt groups and hyperexponential groups.
Mathematika. 2(1955), 21-31.

7 J. Dieudonné, Proceedings of the International Congress of Mathematicians. 1954, Amsterdam.

8 P. Cartier, Groupes formels associés aux anneaux de Witt généralisés.
C.R. Acad.Sc. Paris, t. 265, série A, (1967), 50-52.

9 P. Cartier, Modules associés à un groupe formel commutatif. Courbes typiques.
C.R. Acad.Sc. Paris, t 265, série A, (1967), 129-132.

10 I. Bucur, A. Deleanu, Introduction to the theory of categories and functors.
Wiley-Interscience Publ. 1968.

11 C. Chevalley, Théorie des groupes de Lie, II.
Hermann & Cie, Paris, 1951.

C. R. Acad. Sc. Paris, t. 268, p. 580-582 (17 mars 1969). Série A

ALGÈBRE. — *Sur une série exponentielle non commutative définie sur les corps de caractéristique p.* Note (*) de M. Bert Ditters, transmise par M. Jean Dieudonné.

Le but de cette Note est de donner quelques résultats concernant une série exponentielle non commutative, dite courbe E-pure, dans l'étude des déformations infinitésimales des schémas en groupes. Cette Note ne contient pas de démonstrations; elles seront publiées ultérieurement.

1. Préliminaires. — On note par $\mathbf{F}_p$ le corps premier de caractéristique $p > 0$ et par GCoalg la catégorie de $\mathbf{F}_p$-coalgèbres en groupes. Les objets de cette catégorie sont des $\mathbf{F}_p$-modules A, munis des structures suivantes :

a. un morphisme produit, $m : A \otimes A \to A$, associatif avec unité 1;

b. un morphisme coproduit, $\tau : A \to A \otimes A$, coassociatif, cocommutatif avec coünité ε;

c. la donnée d'un antipodisme $\sigma : A \to A^{opp}$ (algèbre opposée).

Les produits tensoriels sont pris sur $\mathbf{F}_p$; τ, ε et σ sont des homomorphismes pour la structure de $\mathbf{F}_p$-algèbre définie par *a*. Les morphismes, définissant la structure de coalgèbre en groupe sur A doivent satisfaire à la commutativité de certains diagrammes (1).

GCoalg contient l'objet universel $Z = \mathbf{F}_p[Z_1, Z_2, \ldots, Z_n, \ldots]$, l'algèbre polynomiale non commutative graduée, dont le coproduit est donné par la formule de Leibniz $\tau(Z_n) = \sum_{i+j=n} Z_i \otimes Z_j$ (avec $Z_0 = 1$) et dont la graduation ω est définie par $\omega(Z_i) = i$ pour $i \geq 0$ [*cf.* (2), cor. 2 dans le cas commutatif]. En accord avec la notion de courbe, introduite dans (3), on appelle courbe dans G tout morphisme $Z \to G$ dans GCoalg. Une courbe γ dans G est alors donnée par les valeurs $\gamma(Z_i) = x_i$ et l'on écrit $\gamma = \gamma(t) = \sum x_\mu t^\mu$. Si $\gamma(t) = \sum x_\mu t^\mu$, alors pour tout entier $a \geq 1$, $\gamma(t^a) = \sum x_\mu t^{a\mu}$ est encore une courbe. Z étant en même temps un objet « cogroupe » dans GCoalg, le foncteur en ensembles H, défini par $H(G) = GCoalg(Z, G)$ est muni d'une structure de foncteur groupe et la loi de composition de courbes est donnée par multiplication des séries formelles en t avec des coefficients non commutants entre eux. Avec ces notations on a le lemme fondamental suivant :

Lemme 1. — *Il existe un ensemble* $(X_i)_{i \geq 0}$ *d'éléments dans* Z, *tel qu'on ait :*

a. Les X_i *sont isobares de poids* p^i. *Le coefficient de* Z_{p^i} *dans* X_i *est* 1.

b. Il existe des éléments E_μ, $\mu = 0, 1, 2, \ldots$ *dans*

$$U = \mathbf{F}_p[X_0, X_1, \ldots, X_i, \ldots],$$

isobares de poids μ, $E_0 = 1$, $E_{p^i} = X_i$ *pour* $i \geq 0$.

c. $\sum E_\mu t^\mu = \sum E_\mu(X_0, X_1, \ldots)\, t^\mu$ *est une courbe dans* Z.

d. La structure naturelle d'objet de GCoalg sur U *est unique au sens suivant : Si* $\sum F_\mu t^\mu$ *est une courbe dans* Z, *telle que* $F_\mu \in \mathbf{F}_p[F_1, F_{p^1}, \ldots, F_{p^r}, \ldots] = W$ *pour tout* μ *et telle que les* F_μ *sont isobares de poids* μ, *alors il existe un isomorphisme* $U \simeq W$ *dans GCoalg.*

e. U *est minimal au sens suivant : Si* $\sum x_\mu t^\mu \neq 1 . t^0$ *est une courbe dans* Z, *il existe un monomorphisme* $U \to \mathbf{F}_p[x_i]_{i \geq 0}$ *dans GCoalg.*

La situation analogue en caractéristique zéro est bien connue : on retrouve la courbe $\exp(Z_1 t)$ et l'objet U est la bialgèbre du groupe additif.

2. U peut être considéré comme un objet exponentiel et la courbe $\sum E_\mu t^\mu$ comme une série exponentielle en vue des corollaires suivants :

Corollaire 1. — *Soit* $\mathfrak{a}$ *l'idéal bilatère de* U, *engendré par les commutateurs* $[X_i, X_j]$. *Notant* G_μ (resp. Y_i) *les classes de* E_μ (resp. X_i) $\bmod \mathfrak{a}$, *on a* $\sum G_\mu(Y_0, Y_1, \ldots)\, t^\mu = \mathrm{Hex}(Y_0 t, Y_1 t^p, \ldots)$ (2). *En particulier, la série hyperexponentielle définit sur* $A = U/\mathfrak{a}$ *une structure de* $\mathbf{F}_p$*-bialgèbre, qui est identique avec la structure quotient de* $A = U/\mathfrak{a}$ *dans GCoalg.*

Corollaire 2. — *Considérant* $E = \sum E_\mu t^\mu$ *comme élément de* $U[[t]]$, *il existe une* $\mathbf{F}_p[[t]]$*-dérivation* ∂ *de* $U[[t]]$, *telle que* $\partial E_\mu = E_{\mu - 1}$ *et, par conséquent,* $\partial E = E t$.

Corollaire 3. — *Il existe une famille unique* $(V_i)_{i \geq 0} \in Z[[t]]$, *telle que* $\sum Z_\mu t^\mu = E(V_0, V_1, \ldots, V_n, \ldots)$. *On y retrouve la formule de Campbell-Hausdorff-Dieudonné* (3).

Corollaire 4. — *Soient* $B^* \in \mathrm{GCoalg}$ *l'algèbre de distributions sur un groupe formel* B *au sens de Dieudonné et* $x \in \mathrm{Lie}\, B$, *alors il existe une courbe* $\gamma = \sum E_\mu(\xi_0, \xi_1, \ldots, \xi_n, \ldots)\, t^\mu$ *dans* B^* *telle que* $x = \xi_0$. γ *définit un morphisme* $U \to B^*$ *dans GCoalg.*

Soit G dans GCoalg. On appelle courbe E-pure dans G toute courbe $\gamma(t)$ dans G, pour laquelle il existe une famille $(x_i)_{i \geq 0}$ dans G, telle que $\gamma(t) = \sum E_\mu(x_0, x_1, \ldots, x_n, \ldots) t^\mu$. L'auteur doit à P. Gabriel entre autres l'idée d'essayer de démontrer un « théorème de décomposition » pour les courbes. Il a obtenu le résultat suivant :

Théorème (*théorème de décomposition*). — *Soient* G *dans GCoalg et* $\gamma(t)$ *une courbe dans* G. *Alors il existe une famille unique de courbes* E*-pures* γ_j, $j \geq 1$, $(j, p) = 1$ *dans* G *telle que* $\gamma(t) = \prod_{(j,p)=1} \gamma(t^j)$. (*La situation étant non*

commutative en général, il faut que les $\gamma_j(t^j)$ *soient rangés dans l'ordre naturel défini par j.*)

Dans le cas commutatif, ce théorème est bien connu (3).

Il est d'ailleurs équivalent à dire, que la courbe $\sum Z_\mu t^\mu$ est un produit unique des courbes E-pures, ce qui définit une décomposition en somme directe dans GCoalg de Z en copies de U. Remplaçant Z par son sous-objet $Z(r) = \mathbf{F}_p[Z_1, \ldots, Z_r]$, on définit les courbes finies d'ordre r dans $G \in$ GCoalg comme morphismes $Z(r) \to G$ dans GCoalg. Utilisant des conditions d'isobaricité on en déduit, que toute courbe finie dans $G \in$ GCoalg est produit de courbes E-pures finies. Il y a un énoncé analogue au corollaire 4 pour les groupes formels de hauteur finie. Avec les notations du corollaire 4, le théorème de décomposition a le corollaire suivant : *Si* $\dim B = n$, *alors* B^* *admet une p-base ordonnée* $(x_{ij})_{i \geq 0, 1 \leq j \leq n}$, *telle que les* $(x_{ij})_{i \geq 0}$ *définissent des courbes* E-*pures.*

(*) Séance du 24 février 1969.
(1) P. Gabriel, *S. G. A. D.* '63-'64, Exp. VII^A, § 3.
(2) P. Cartier, *Comptes rendus*, 265, série A, 1967, p. 50.
(3) P. Cartier, *Comptes rendus*, 265, série A, 1967, p. 129.
(4) J. Dieudonné, *Matematika*, 2, 1955, p. 21-31.
(5) J. Dieudonné, *Bull. Soc. math. Fr.*, 84, 1956, p. 239.

(*Mathematisch Instituut,*
Katholieke Universiteit,
Nijmegen, Pays-Bas.)

179351. — Imp. GAUTHIER-VILLARS. — 55, Quai des Grands-Augustins, Paris (6e).
Imprimé en France.

SAMENVATTING

Deze studie is gewijd aan de theorie van formele groepen, gedefiniëerd over een willekeurig grondlichaam. Het bouwt voort op het werk dat met name door J.A. Dieudonné op dit terrein verricht is. De exp-afbeelding in de klassieke theorie, waar het grondlichaam het lichaam der complexe getallen is, blijkt een analogon te hebben, wanneer het grondlichaam positieve karakteristiek heeft. Deze analogie wordt bestudeerd (hoofdstuk 2 en 3). Tenslotte worden in hoofdstuk 4 enige gebieden voor verdere studie aangegeven. De resultaten van de eerste drie hoofdstukken zijn verschenen in een Note in de Comptes Rendus (C.R. Acad.Sc. Paris, t. 268, Série A, 1969, 580-582).

STELLINGEN

1 Zij $\mathfrak{g}$ een Liealgebra over een lichaam van karakteristiek 0 en zij $U(\mathfrak{g})$ de omhullende algebra van $\mathfrak{g}$. Gezien de resultaten van dit proefschrift zijn de groep $H(U(\mathfrak{g}))$, (1.4.8) en de afbeelding $\mathfrak{g} \to H(U(\mathfrak{g}))$, $x \mapsto \exp xt$ voor de hand liggende hulpmiddelen om de theorie van locale Liegroepen te beschrijven.

2 Zij A het grootste abelse quotient van de NEG, (dit proefschrift (3.1.8)), en zij $\hat{A}$ de completering van A in de oorsprong. Dan is er een natuurlijk isomorfisme $\hat{A} \simeq A^*$. Dit kan gebruikt worden voor een numerieke explicitering van Cartierdualiteit.

3 Zij $g : V \to W$ een morfisme van irreducibele algebraïsche variëteiten. De verzameling punten $p \in V$, waarvoor de raakafbeelding $\mathrm{grad}_p(g)$ injectief is, is open in V. Dit geeft een vereenvoudiging van een stelling van Chevalley.

(Classification des groupes de Lie algébriques, Exp 15).

4 De cohomologiering met gehele coëfficienten van de ruimte der lussen op een complexe projectieve ruimte kan ook met behulp van meetkundige overwegingen worden bepaald.

5 Een semigroep met nuldimensionale topologie, die compact is in deze topologie, is projectieve limiet van eindige semigroepen.

6 Het bewijs van de stelling van Riemann-Roch, zoals dit gegeven wordt door A. Pfluger, is onjuist.

(A. Pfluger, Theorie der Riemannschen Flächen, Springer Verlag, 1957).

7 Een van de grote dilemma's omtrent muzikale interpretatie wordt opgelost als men antwoord weet op de vraag: Moet men de Ordres van Fr. Couperin op een electrisch versterkt clavecimbel spelen in de oorspronkelijke vingerzetting?

8 Een recent onderzoek over kabbalistiek leidt tot de conclusie dat J.S. Bach behalve als eminent componist ook als bekwaam getaltheoreticus beschouwd moet worden. Een partituur van Das Wohltemperierte Klavier dient dan ook in een goed geoutilleerde mathematische bibliotheek niet te ontbreken.

(H. Brandts Buys.
Het Wohltemperirte Klavier van Johann Sebastian Bach. Arnhem 1955).